

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

أو نشرها من خلال القنوات العامة.

السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للتُغرات المسجلة national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology the National Institute of Standards and Technology (NIST) من قبل (NIST) National Vulnerability Database (NVD) for the week from 26th الأسبوع من ٢٦ مارس إلى National Vulnerability Database (NVD) of March to 1st of April. Vulnerabilities are scored using the Common معيار معيار معيار أبريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Vulnerability Scoring System (CVSS) standard as per the following حيث يتم تصنيف الثغرات بناء على Vulnerability Scoring System (CVSS) severity:

Critical: CVSS base score of 9.0-10.0 High: CVSS base score of 7.0-8.9 Medium: CVSS base score 4.0-6.9 Low: CVSS base score 0.0-3.9

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء As part of NCA duties to help securing the cyberspace and protecting التالي:

عالى جدًا: النتيجة الأساسية لـ10.0-CVSS 9.0

عالى: النتيجة الأساسية لـ8.9-7.0 CVSS

متوسط: النتيجة الأساسية لـ6.9-CVSS 4.0

منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	Score	Severity
		Some smartphones have configuration issues. Successful			
	huawei - multiple	exploitation of this vulnerability may cause kernel privilege			
CVE-2022-48353	products	escalation, which results in system service exceptions.	2023-03-27	9.8	Critical
	· 	Vendor: The Apache Software Foundation Versions Affected:			
	apache -	Apache OpenMeetings from 2.0.0 before 7.0.0 Description:			
CVE-2023-28326	openmeetings	Attacker can elevate their privileges in any room	2023-03-28	9.8	Critical
		This vulnerability allows remote attackers to bypass authentication			
		on affected installations of Ivanti Avalanche 6.3.2.3490. The			
		specific flaw exists within the ProfileDaoImpl class. A crafted			
		request can trigger execution of SQL queries composed from a			
		user-supplied string. An attacker can leverage this vulnerability to			
CVE-2022-36972	ivanti - avalanche	bypass authentication on the system. Was ZDI-CAN-15328.	2023-03-29	9.8	Critical
		This vulnerability allows remote attackers to execute arbitrary			
		code on affected installations of Ivanti Avalanche 6.3.2.3490.			
		Although authentication is required to exploit this vulnerability,			
		the existing authentication mechanism can be bypassed. The			
		specific flaw exists within the Web File Server service. The issue			
		results from the lack of proper validation of user-supplied data,			
		which can result in deserialization of untrusted data. An attacker			
		can leverage this vulnerability to execute code in the context of			
CVE-2022-36974	ivanti - avalanche	the service account. Was ZDI-CAN-15330.	2023-03-29	9.8	Critical
		This vulnerability allows remote attackers to bypass authentication			
		on affected installations of Ivanti Avalanche 6.3.2.3490. The			
		specific flaw exists within the ProfileDaoImpl class. A crafted			
		request can trigger execution of SQL queries composed from a			
		user-supplied string. An attacker can leverage this vulnerability to			
<u>CVE-2022-36975</u>	ivanti - avalanche	bypass authentication on the system. Was ZDI-CAN-15332.	2023-03-29	9.8	Critical
		This vulnerability allows remote attackers to bypass authentication			
		on affected installations of Ivanti Avalanche 6.3.2.3490. The			
		specific flaw exists within the GroupDaoImpl class. A crafted			
		request can trigger execution of SQL queries composed from a			
		user-supplied string. An attacker can leverage this vulnerability to			
CVE-2022-36976	ivanti - avalanche	bypass authentication on the system. Was ZDI-CAN-15333.	2023-03-29	9.8	Critical
		This vulnerability allows remote attackers to execute arbitrary			
		code on affected installations of Ivanti Avalanche 6.3.2.3490.			
		Although authentication is required to exploit this vulnerability,			
		the existing authentication mechanism can be bypassed. The			
		specific flaw exists within the Certificate Management Server			
		service. The issue results from the lack of proper validation of			
		user-supplied data, which can result in deserialization of untrusted			
0.45 0.005 5.55=	l	data. An attacker can leverage this vulnerability to execute code in			
CVE-2022-36977	ivanti - avalanche	the context of the service account. Was ZDI-CAN-15449.	2023-03-29	9.8	Critical
		This vulnerability allows remote attackers to execute arbitrary			
		code on affected installations of Ivanti Avalanche 6.3.2.3490.			
		Although authentication is required to exploit this vulnerability,			
		the existing authentication mechanism can be bypassed. The			
CVE 2022 2022	ivanti - avalanche	specific flaw exists within the Notification Server service. The issue results from the lack of proper validation of user-supplied data,	2022 02 20	0.0	Californi
CVE-2022-36978	IVANTI - AVAIANCHA	I results from the lack of brober validation of liser-subblied data	2023-03-29	9.8	Critical

Г		The second secon			
		which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of			
		the service account. Was ZDI-CAN-15448.			
		This vulnerability allows remote attackers to bypass authentication			
		on affected installations of Ivanti Avalanche 6.3.2.3490. Although	ļ		
		authentication is required to exploit this vulnerability, the existing			
		authentication mechanism can be bypassed. The specific flaw			
		exists within the AvalancheDaoSupport class. A crafted request			
		can trigger execution of SQL queries composed from a user-	ļ		
CVE 2022 20070	iventi evelende	supplied string. An attacker can leverage this vulnerability to	2022 02 20	0.0	Cuitinal
CVE-2022-36979	ivanti - avalanche	bypass authentication on the system. Was ZDI-CAN-15493.	2023-03-29	9.8	Critical
		This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche 6.3.3.101.			
		Although authentication is required to exploit this vulnerability,	ļ		
		the existing authentication mechanism can be bypassed. The	ļ		
		specific flaw exists within the DeviceLogResource class. The issue			
		results from the lack of proper validation of a user-supplied path	ļ		
		prior to using it in file operations. An attacker can leverage this	ļ		
		vulnerability to execute code in the context of the service account.			
CVE-2022-36981	ivanti - avalanche	Was ZDI-CAN-15966.	2023-03-29	9.8	Critical
<u>CVL 2022 30301</u>	ivanti avaiantine	This vulnerability allows remote attackers to bypass authentication	2023 03 23	3.0	Circical
		on affected installations of Ivanti Avalanche 6.3.3.101.	ļ		
		Authentication is not required to exploit this vulnerability. The			
		specific flaw exists within the SetSettings class. The issue results			
		from the lack of authentication prior to allowing access to			
		functionality. An attacker can leverage this vulnerability to bypass			
CVE-2022-36983	ivanti - avalanche	authentication on the system. Was ZDI-CAN-15919.	2023-03-29	9.8	Critical
<u>CVL 2022 30303</u>	ivanti avaiantine	The MediaProvider module has a vulnerability of unauthorized	2023 03 23	3.0	Citical
	huawei - multiple	data read. Successful exploitation of this vulnerability may affect			
CVE-2022-48348	products	confidentiality and integrity.	2023-03-27	9.1	Critical
<u>CVL 2022 103 10</u>	products	The control component has a spoofing vulnerability. Successful	2023 03 27	J.1	Circical
	huawei - multiple	exploitation of this vulnerability may affect confidentiality and			
CVE-2022-48349	products	availability.	2023-03-27	9.1	Critical
<u> </u>	p. 0 d. d. 0 d	Deserialization of Untrusted Data vulnerability in Apache Software			0.10.00.
		Foundation Apache InLong. It could be triggered by authenticated	ļ		
		users of InLong, you could refer to [1] to know more about this			
		vulnerability. This issue affects Apache InLong: from 1.1.0 through	ļ		
		1.5.0. Users are advised to upgrade to Apache InLong's latest	ļ		
		version or cherry-pick [2] to solve it. [1]	ļ		
		https://programmer.help/blogs/jdbc-deserialization-vulnerability-			
		learning.html https://programmer.help/blogs/jdbc-deserialization-			
		vulnerability-learning.html [2]			
		https://github.com/apache/inlong/pull/7422	ļ		
CVE-2023-27296	apache - inlong	https://github.com/apache/inlong/pull/7422	2023-03-27	8.8	High
	· ·	This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of TP-Link AC1750 prior to	ļ		
		211210 routers. Authentication is not required to exploit this	ļ		
		vulnerability. The specific flaw exists within the NetUSB.ko kernel			
		module. The issue results from the lack of proper validation of	ļ		
		user-supplied data, which can result in a read past the end of an			
	tp-link -	allocated buffer. An attacker can leverage this vulnerability to			
CVE-2022-24352	ac1750_firmware	execute code in the context of root. Was ZDI-CAN-15773.	2023-03-28	8.8	High
		This vulnerability allows network-adjacent attackers to execute	7		
		arbitrary code on affected installations of TP-Link AC1750 1.1.4			
		Build 20211022 rel.59103(5553) routers. Authentication is not			
		required to exploit this vulnerability. The specific flaw exists within			
		the NetUSB.ko module. The issue results from the lack of proper			
		validation of user-supplied data, which can result in a read past			
		the end of an allocated buffer. An attacker can leverage this			
	tp-link -	vulnerability to execute code in the context of the root user. Was	·	_	
CVE-2022-24353	ac1750_firmware	ZDI-CAN-15769.	2023-03-28	8.8	High
		A vulnerability has been reported to affect multiple QNAP			
		operating systems. If exploited, the vulnerability allows remote			
		authenticated users to execute arbitrary commands via			
		susceptible QNAP devices. The vulnerability affects the following			
		QNAP operating systems: QTS, QuTS hero, QuTScloud, QVP (QVR			
		Pro appliances), QVR. We have already fixed the vulnerability in			
		the following operating system versions: QTS 5.0.1.2346 build			
	qnap - multiple	20230322 and later QuTS hero h5.0.1.2348 build 20230324 and	·	_	
CVE-2023-23355	products	later	2023-03-29	8.8	High
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of NETGEAR R6700v3			
		1.0.4.120_10.0.91 routers. Authentication is not required to			
		exploit this vulnerability. The specific flaw exists within the NetUSB			
		module. The issue results from the lack of proper validation of			
		user-supplied data, which can result in an integer overflow before			
	and the second s	The second secon	1		
CVE-2022-27641	netgear - d7800_firmware	allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15806.	2023-03-29	8.8	High

	T	T			
		This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700v3			
		1.0.4.120_10.0.91 routers. Authentication is not required to			
		exploit this vulnerability. The specific flaw exists within the httpd			
		service. The issue results from incorrect string matching logic			
		when accessing protected pages. An attacker can leverage this in			
	netgear -	conjunction with other vulnerabilities to execute code in the			
CVE-2022-27642	cax80_firmware	context of root. Was ZDI-CAN-15854.	2023-03-29	8.8	High
	_	This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of NETGEAR R6700v3			
		1.0.4.120_10.0.91 routers. Authentication is not required to			
		exploit this vulnerability. The specific flaw exists within the			
		handling of SOAP requests. When parsing the SOAPAction header,			
		the process does not properly validate the length of user-supplied			
		data prior to copying it to a buffer. An attacker can leverage this			
	netgear -	vulnerability to execute code in the context of root. Was ZDI-CAN-			
CVE-2022-27643	r6400_firmware	15692.	2023-03-29	8.8	High
		This vulnerability allows network-adjacent attackers to			
		compromise the integrity of downloaded information on affected			
		installations of NETGEAR R6700v3 1.0.4.120_10.0.91 routers.			
		Authentication is not required to exploit this vulnerability. The			
		specific flaw exists within the downloading of files via HTTPS. The			
		issue results from the lack of proper validation of the certificate			
	netgear -	presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in			
CVE-2022-27644	r6400 firmware	the context of root. Was ZDI-CAN-15797.	2023-03-29	8.8	High
<u> </u>	10-100_IIIIIIWale	This vulnerability allows network-adjacent attackers to bypass	2023 UJ-23	5.5	111811
		authentication on affected installations of NETGEAR R6700v3			
		1.0.4.120 10.0.91 routers. Authentication is not required to			
		exploit this vulnerability. The specific flaw exists within			
		readycloud_control.cgi. The issue results from incorrect string			
		matching logic when accessing protected pages. An attacker can			
	netgear -	leverage this vulnerability to execute code in the context of root.			
CVE-2022-27645	lax20_firmware	Was ZDI-CAN-15762.	2023-03-29	8.8	High
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of NETGEAR R6700v3			
		1.0.4.120_10.0.91 routers. Although authentication is required to			
		exploit this vulnerability, the existing authentication mechanism			
		can be bypassed. The specific flaw exists within the circled			
		daemon. A crafted circleinfo.txt file can trigger an overflow of a			
		fixed-length stack-based buffer. An attacker can leverage this			
01/5 2022 27646	netgear -	vulnerability to execute code in the context of root. Was ZDI-CAN-	2022 02 22	0.0	
CVE-2022-27646	r6400_firmware	15879.	2023-03-29	8.8	High
		This vulnerability allows remote attackers to execute arbitrary code on affected installations of Ivanti Avalanche 6.3.2.3490.			
		Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The			
		specific flaw exists within the JwtTokenUtility class. The issue			
		results from the lack of proper validation of user-supplied data,			
		which can result in deserialization of untrusted data. An attacker			
		can leverage this vulnerability to execute code in the context of			
CVE-2022-36971	ivanti - avalanche	the service account. Was ZDI-CAN-15301.	2023-03-29	8.8	High
		This vulnerability allows remote attackers to bypass authentication			
		on affected installations of Ivanti Avalanche 6.3.2.3490. Although			
		authentication is required to exploit this vulnerability, the existing			
		authentication mechanism can be bypassed. The specific flaw			
		exists within the ProfileDaoImpl class. A crafted request can trigger			
		execution of SQL queries composed from a user-supplied string.			
01/2 0000 000		An attacker can leverage this vulnerability to bypass	2000 5	•	
CVE-2022-36973	ivanti - avalanche	authentication on the system. Was ZDI-CAN-15329.	2023-03-29	8.8	High
		This vulnerability allows network-adjacent attackers to bypass			
		authentication on affected installations of D-Link DIR-1935 1.03			
		routers. Authentication is not required to exploit this vulnerability.			
		The specific flaw exists within the handling of HNAP login requests.			
		The issue results from the lack of proper implementation of the			
	d-link - multiple	authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-			
CVE-2022-43620	products	CAN-16142.	2023-03-29	8.8	High
CVL 2022-43020	products	This vulnerability allows network-adjacent attackers to bypass	2023-03-23	0.0	111811
		authentication on affected installations of D-Link DIR-1935 1.03			
		routers. Authentication is not required to exploit this vulnerability.			
		The specific flaw exists within the handling of HNAP login requests.			
		The issue results from an incorrectly implemented comparison. An			
	d-link - multiple	attacker can leverage this vulnerability to bypass authentication			
CVE-2022-43621	products	on the system. Was ZDI-CAN-16152.	2023-03-29	8.8	High
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of D-Link DIR-1935 1.03			
		routers. Authentication is not required to exploit this vulnerability.			
	d-link - multiple	The specific flaw exists within the handling of Login requests to the			
CVE 2022 42622	products	web management portal. When parsing the HNAP_AUTH header,	2023-03-29	8.8	High
CVE-2022-43622	p. 0 a.a.010				

			T	1	
		the process does not properly validate the length of user-supplied			
		data prior to copying it to a fixed-length stack-based buffer. An			
		attacker can leverage this vulnerability to execute code in the			
		context of root. Was ZDI-CAN-16139.			
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Authentication is not required to exploit this vulnerability.			
		, , ,			
		The specific flaw exists within the handling of http requests to the web management portal. When parsing the SOAPAction header,			
		the process does not properly validate the length of user-supplied			
		data prior to copying it to a fixed-length stack-based buffer. An			
	d-link - multiple	attacker can leverage this vulnerability to execute code in the			
CVE-2022-43630	products	context of root. Was ZDI-CAN-16150.	2023-03-29	8.8	High
CVL 2022 +3030	products	This vulnerability allows network-adjacent attackers to bypass	2023 03 23	0.0	111811
		authentication on affected installations of TP-Link TL-WR940N			
		6_211111 3.20.1(US) routers. Authentication is not required to			
		exploit this vulnerability. The specific flaw exists within the httpd			
		service, which listens on TCP port 80 by default. The issue results			
		from the lack of sufficient randomness in the sequnce numbers			
		used for session managment. An attacker can leverage this			
	tp-link - tl-	vulnerability to bypass authentication on the system. Was ZDI-			
CVE-2022-43636	wr940n firmware	CAN-18334.	2023-03-29	8.8	High
	<u>-</u>	Server-Side Request Forgery (SSRF) vulnerability in Apache			<u></u>
		Software Foundation Apache Fineract. Authorized users with			
		limited permissions can gain access to server and may be able to			
		use server for any outbound traffic. This issue affects Apache			
CVE-2023-25195	apache - fineract	Fineract: from 1.4 through 1.8.3.	2023-03-28	8.1	High
		This vulnerability allows remote attackers to bypass authentication			
		on affected installations of Ivanti Avalanche 6.3.2.3490. Although			
		authentication is required to exploit this vulnerability, the existing			
		authentication mechanism can be bypassed. The specific flaw			
		exists within the EnterpriseServer service. The issue results from			
		the lack of proper locking when performing operations during			
		authentication. An attacker can leverage this vulnerability to			
CVE-2022-36980	ivanti - avalanche	bypass authentication on the system. Was ZDI-CAN-15528.	2023-03-29	8.1	High
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of TP-Link TL-WR940N			
		3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is			
		required to exploit this vulnerability. The specific flaw exists within			
		the httpd service, which listens on TCP port 80 by default. The			
		issue results from the lack of proper validation of the length of			
		user-supplied data prior to copying it to a fixed-length stack-based			
	tp-link - tl-	buffer. An attacker can leverage this vulnerability to execute code			
CVE-2022-0650	wr940n_firmware	in the context of root. Was ZDI-CAN-13993.	2023-03-28	8	High
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of TP-Link TL-WR940N			
		3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is			
		required to exploit this vulnerability. The specific flaw exists within			
		the httpd service, which listens on TCP port 80 by default. The			
		issue results from the lack of proper validation of the length of			
	1. 10. 1	user-supplied data prior to copying it to a fixed-length stack-based			
CVE 2022 24272	tp-link - tl-	buffer. An attacker can leverage this vulnerability to execute code	2022 02 22		119 . 1.
CVE-2022-24973	wr940n_firmware	in the context of root. Was ZDI-CAN-13992.	2023-03-28	8	High
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of NETGEAR R6700v3			
		1.0.4.120_10.0.91 routers. Although authentication is required to			
		exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the			
		name or email field provided to libreadycloud.so. The issue results			
		from the lack of proper validation of a user-supplied string before			
		using it to execute a system call. An attacker can leverage this			
	netgear -	vulnerability to execute code in the context of root. Was ZDI-CAN-			
CVE-2022-27647	cax80 firmware	15874.	2023-03-29	8	High
<u> </u>	- cando_mmware	This vulnerability allows network-adjacent attackers to execute	2023 03-23	U	111611
		arbitrary code on affected installations of TP-Link TL-WR841N TL-			
		WR841N(US) V14 220121 routers. Although authentication is			
		required to exploit this vulnerability, the existing authentication			
		mechanism can be bypassed. The specific flaw exists within the			
		ated_tp service. The issue results from the lack of proper			
		validation of a user-supplied string before using it to execute a			
	tp-link - tl-	system call. An attacker can leverage this vulnerability to execute			
CVE-2022-42433	wr841_firmware	code in the context of root. Was ZDI-CAN-17356.	2023-03-29	8	High
		In the Linux kernel, pick_next_rt_entity() may return a type			
		confused entry, not detected by the BUG_ON condition, as the			
		confused entry will not be NULL, but list_head.The buggy error			
		condition would lead to a type confused entry with the list			
		head,which would then be used as a type confused			
CVE-2023-1077	linux - linux_kernel	sched_rt_entity,causing memory corruption.	2023-03-27	7.8	High
	anan_ncirie	1 12 24 - 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2			٠٠٠٥''

Sockes) protected. The city or protected protect of the country of		<u> </u>	A (I			
Bid_entity on the head of a list classing a type controllan. Local user can trigger that with sty, message put, Type controllands and to 'struct' ridg, mag, sooy, info' info' actually point to something electrons are controlled to 'struct' ridg, mag, sooy, info' info' actually point to something electrons are controlled to 'struct' ridg, mag, sooy, info' info' actually point to something electrons are controlled to 'struct' ridger info 'struct'			A flaw was found in the Linux Kernel in RDS (Reliable Datagram			
user can risigant this with mist, message_multi. Type contaisant leads to struct risk, mag. Toxype_mid miniod scalable points to something else that is potentially controlled by local user. It is known how to trager cisk, which causes and or of houses access, and allock. 2023-08-27 7.8 Might adobbe substance_30_stsp adobbe substance_30_stsp er Adobbe substance_30_stsp er Substance_30_stsp						
else that is potentially composed by local user. It is known how to regiger this, which cause an out of bounds access, and a lock compution. Addies Substance 30 Stager versions 2.0.0 (and certifier) are affected by an out of bounds read witherability when parsing a discated memory variature. An attacker could leverage life variability of security or variature. An attacker could leverage life variability of security or variature. An attacker could leverage life variability of security or variature. An attacker could leverage life variability of security or variature. An attacker could leverage life. VEF 2023-23864 or er Addie Substance 30 Stager versions 2.0.0 (and earlier) are affected by a relap-based whife Covertion vulnerability that could result in must open a malicious file. VEF 2023-23864 or er Addies Substance 30 Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in a distance 30 Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in a distance 30 Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in a distance 30 Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in a distance 30 Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. VEF 2023-23867 or er Adobe Substance 30 Stager versions 2.0.0 (and earlier) are affected by an inchange of this issue requires user interaction in that a victim must open a malicious file. VEF 2023-23860 or er Adobe Substance 30 Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a substance 30 Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds						
trigger the, which causes an out of bounds access, and a lock corruption. Adobe Substance 3D Stager versions 2.00 (and earlier) are substance 3D Stager versions 2.00 (and ea			,.			
Adobe Substance 30 Stager versions 2.0.0 land carrier1 are affected by an out-of-bounds read vulnerability when parsing a carter field by an out-of-bounds read vulnerability when parsing a carter field by an out-of-bounds read vulnerability when parsing a carter field by an out-of-bounds read vulnerability when parsing a carter field by an out-of-bounds read vulnerability when parsing a carter field by an out-of-bounds read vulnerability when parsing a carter field by a first part of the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by a literap-based flaffer Overflow vulnerability that rould result in a shiftancy code execution in the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are substance 3d Stager versions 2.0.0 and earlier] are affected by a interpore input Validation vulnerability that rould result in a shiftancy code execution in the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by an out-of-bounds with vulnerability that rould result in a shiftancy code execution in the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by an out-of-bounds with vulnerability that rould result in a shiftancy code execution in the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by an out-of-bounds with vulnerability that rould result in a shiftancy code execution in the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by an out-of-bounds with vulnerability that rould result in a shiftancy code execution in the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by an out-of-bounds with the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by an out-of-bound with the context of the current user. Substance 3d Stager versions 2.0.0 and earlier] are affected by an ideal shape an affected by an ideal shape an a						
Adobb Substance 3D Staget versions 2.0 0 and earlier) are affected by an out-of-bounder seal uniterated users in a read past the end of an adobb-substance 3d staget versions 2.0 0 and earlier) are substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. Substance 3d staget versions 2.0 in the context of the current user. S	CVF-2023-1078	linux - linux kernel		2023-03-27	7.8	High
corlect file, which could result in a read past the read of an inflorated memory structure. An attacker could leverage this varientability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adoba- substance 3 of stage versions 2 0.0 (and earlier) are all case of by a rivery based fisher (overflow vulnerability that could result in must open a malicious file. Adoba- substance 3 of stage versions 2.0 (and earlier) are substance, 3 of stage versions 2.0 (and e	<u> </u>	iniax iniax_kerrier		2023 03 27	7.0	6
allocated memory structure. An attacker could leverage this value and the substance 3 distance 3 di			The state of the s			
adobe - substance, 3d, stage CVE-2023-25865			·			
substance, 3d, stag. CVE-2023-25864 er Adobe Substance 30 Stager versions 2.0.0 (and earlier) are affected by an analizous file. CVE-2023-25865 CVE-2023-25866 er Adobe Substance 30 Stager versions 2.0.0 (and earlier) are affected by an analizous file. CVE-2023-25867 CVE-2023-25867 CVE-2023-25871 CVE-2023-25871 CVE-2023-25872 CVE-2023-2		a dala a	_			
must open a malicious file. Adobe Substance 30 Stager versions 2.0.0 (and earlier) are affected by a heap-based furfer Overflow underability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. OVE 2023 25865 OVE 2023 25866 OVE 2023 25867 OVE 2023 25867 OVE 2023 25868 OVE 2023 25871 OVE 2023 25872 OVE 2023 25873 OVE 2023 25872 OVE 2023 25873 OVE 2023 25874 OVE 2023 25			·			
Adobe substance 30 Stager versions 2.0.0 and earlier) are affected by a responsed miller (overflow witnershillty that could result in arbitrary code execution in the context of the current service in the context of the current services. But a replication of this issue requires user interaction in that a victim must open a malicious file. QVE.2023-25865 QVE.2023-25865 QVE.2023-25865 QVE.2023-25866 QVE.2023-25867 QVE.2023-25866 QVE.2023-25866 QVE.2023-25867 QVE.2023-25866 QVE.2023-25867 QVE.2023-25866 QVE.2023-25867 QVE.2023-25866 QVE.2023-25867 QVE.2023-25866 QVE.2023-25867 QVE.2023-25867 QVE.2023-25868 QVE.2023-25867 QVE.2023-25868 QVE.2023-25868 QVE.2023-25868 QVE.2023-25869 QVE.2023-25869 QVE.2023-25869 QVE.2023-25869 QVE.2023-25869 QVE.2023-25869 QVE.2023-25869 QVE.2023-25869 QVE.2023-25870 QVE.2023-	CVE-2023-25863		· ·	2023-03-27	7.8	High
adobe - subtance, 3d, stage						
week for the part of the save requires user interaction in that a victim must pen a malicious file. VE-2023-25867 CVE-2023-25867 CVE-2023-25867 CVE-2023-25868 CVE-2023-25869 CVE-2023-25870 CVE-2023-25871 CVE-2023-25871 CVE-2023-25871 CVE-2023-25872 CVE-2023-25872 CVE-2023-25873 CVE-2023-25873 CVE-2023-25874 CVE-2023-25874 CVE-2023-25874 CVE-2023-25874 CVE-2023-25874 CVE-2023-25874 CVE-2023-25875 CVE-2023-25876 CVE-2023-25877 CVE-2023-2						
CVE-2023-25856 er victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a malicious file. 2023-03-27 7.8 High adobe - victim must open a ma			•			
Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Expolatation of this issue requires user interaction in that a victim must open amalicous file. VE-2023-25865 CVE-2023-25865 CVE-2023-25866 CVE-2023-25866 CVE-2023-25867 CVE-2023-25867 CVE-2023-25867 Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Expolatation of this issue requires user interaction in that a victim must open amalicous file. CVE-2023-25867 CVE-2023-25867 CVE-2023-25868 CVE-2023-25868 CVE-2023-25869 CVE-2023-25870 CVE-2023-25871 CVE-2023-25872 CVE-2023-25872 CVE-2023-25872 CVE-2023-25872 CVE-2023-25873 CVE-2023-25874 CVE-2023-25874 CVE-2023-25877 CVE-2023-25	CVF-2023-25864		·	2023-03-27	7.8	High
adobe - substance_3d_stage cyte_2023_25865 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25866 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25867 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25867 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25872 er Adobe Substance 3D_stager versions 2.0.0 (and earlier) are 2023_03.277 7.8 High cyte_2023_25872 e	CVL-2023-23604	eı		2023-03-27	7.6	riigii
substance_3d_stag victim must open a malicious file. QVE-2023-25869 CVE-2023-25869 CVE-2023-25879 Adobe Substance 30 Stager versions 2.0.0 (and earlier) are affected by an unit of bounds write witheraction in that a victim must open a malicious file. Adobe Substance 30 Stager versions 2.0.0 (and earlier) are affected by an unit of bounds read vinerability when parsing a crafted file, which could result in arbitrary code execution in the context of the current service by a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this ready and the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25870 CVE-2023-25870 CVE-2023-25870 CVE-2023-25870 CVE-2023-25871 CVE-2023-25871 CVE-2023-25872 CVE-2023-25872 CVE-2023-25873 CVE-2023-25873 CVE-2023-25873 CVE-2023-25874 CVE-2023-25874 CVE-2023-25875 CVE-2023-25877 CVE-2023-25878 CVE-2023-25878 CVE-2023-25878 CVE-2023-25878 CVE-2023-25878 CVE-2023-25878 CVE-2023-25878 CVE			· · · · · · · · · · · · · · · · · · ·			
CVE-2023-25869 er wictim must open a malicious file. 2023-03-27 7.8 High adobe substance 3d stage control for the current user. Substance 3d stage control for the current user substance 3d stage control for the current user. Substance 3d stage control for the current user substance 3d stage control for the current user. Substance 3d stage substance 3d stage control for the current user. Substance 3d stage substance 3d stage substance 3d stage substance 3d stage control for the current user. Substance 3d stage substa		adobe -	,			
Adobe Substance 3.0 Stager versions 2.0.0 (and earlier) are affected by an out-of bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Substance, 3d, stag. CVE-2023-25867 CVE-2023-25868 CVE-2023-25869 CVE-2023-25869 Adobe Substance 3.0 Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in arbitrary code execution in the context of the current suser. Substance, 3d, stag. CVE-2023-25869 CVE-2023-25869 CVE-2023-25869 CVE-2023-25869 Adobe Substance 3.0 Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in arbitrary code execution in the context of the current suser affected by a learn based before the current suser in the context of the current suser affected by a learn based before the current suser in the context of the current suser affected by an out-of-bounds read vulnerability when parsing a crafted life which could result in arbitrary code execution in the context of the current suser substance, 3d, stag in a craft of the village versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted life which could result in a read pars the end of an adobe-substance 3d, stag in a read part of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25870 Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25871 Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malic	0.45 0000 05005					
adobe- substance_3d_stag EVE-2023-25867 CVE-2023-25867 CVE-2023-25867 CVE-2023-25867 Adobe_Substance_3d_stag CVE-2023-25867 CVE-2023-25868 CVE-2023-25869 Adobe_Substance_3d_stag CVE-2023-25869 CVE-2023-25869 CVE-2023-25869 Adobe_Substance_3d_stag CVE-2023-25869 CVE-2023-25869 CVE-2023-25869 Adobe_Substance_3d_stag CVE-2023-25869 CVE-2023-25869 CVE-2023-25869 Adobe_Substance_3d_stag CVE-2023-25869 CVE-2023-25869 Adobe_Substance_3d_stag CVE-2023-25869 CVE-2023-25869 Adobe_Substance_3d_stag CVE-2023-25870 Adobe_Substance_3d_stag CVE-2023-25872 Adobe_Substance_3d_stag CVE-2023-25873 Adobe_Substance_3d_stag CVE-2023-25873 Adobe_Substance_3d_stag CVE-2023-25874 Adobe_Substance_3d_stag CVE-2023-2587	CVE-2023-25865	er		2023-03-27	7.8	High
adobe - substance_3d_stag CVE-2023-25866 er Adobe Substance 13 Stager versions 2.0.0 (and earlier) are affected by an Improper input Validation witheraction in that a victim must open a malicious file. CVE-2023-25869 er Adobe Substance 3D stager versions 2.0.0 (and earlier) are affected by an Improper input Validation witherability that could result in arbitrary code execution in the context of the current version in that a victim must open a malicious file. CVE-2023-25869 er Adobe Substance 3D stager versions 2.0.0 (and earlier) are affected by an Out-of-bounds water valunerability when parsing a crafted by an out-of-bounds with valunerability that could result in arbitrary code execution in the context of the current version substance_3d_stag VVE-2023-25870 er Adobe Substance 3D stager versions 2.0.0 (and earlier) are affected by an out-of-bounds water valunerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability and the particular of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25870 er Adobe Substance 3D stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25871 er Adobe Substance 3D stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873						
substance_3d_state er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could adobe - substance_3d_state er Adobe Substance_3D Stager versions 2.0.0 (and earlier) are affected by an improper input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. OVE-2023-25868 EVE-2023-25868 EVE-2023-25869 EVE-2023-25870 EVE-2023-25870 EVE-2023-25870 EVE-2023-25870 EVE-2023-25871 EVE-2023-25871 EVE-2023-25871 EVE-2023-25872 EVE-2023-25873 EVE-2023-25874 EVE-2023-25874 EVE-2023-25874 EVE-2023-25874 EVE-2023-25875 EVE-2023-25875 EVE-2023-25876 EVE-2023-25876 EVE-2023-25877 EVE-2023-25877 EVE-2023-25878 EVE-2023-25878 EVE-2023-25878 EVE-2023-25878 EVE-2023-25878 EVE-2023-25879 EVE-2023-25879 EVE-2023-25879 EVE-2023-25870 EVE-202		adobe -				
Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an Improper Input Validation whereability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25869 CVE-2023-25870 CVE-2023-25870 CVE-2023-25870 CVE-2023-25870 CVE-2023-25871 CVE-2023-25871 CVE-2023-25872 CVE-2023-25874 CVE-2023		substance_3d_stag	Exploitation of this issue requires user interaction in that a victim			
adobe - substance 3d_stage	CVE-2023-25866	er	·	2023-03-27	7.8	High
cyE-2023-25867 er substance 3d_stage substance 3d_stage versions 2.0.0 (and earlier) are substance 3d_stage versions 2.0.0 (and earlier) are affected by a leap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current such adobe - substance 3d_stage versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in arbitrary code execution in the context of the current such affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Substance 3d_stage and adobe - substance 3d_stage versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Substance 3d_stage versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25870 er must open a malicious file. CVE-2023-25871 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er displayed to the substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er er vicin must open a malicious file. CVE-2023-25874 er vicin must open a malicious file. CVE-2023-25874 er vici						
substance_3d_stag		adobe -				
wittim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25869 CVE-2023-25872 er victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a rabitrary code execution in that a victim must open a malicious file. QVE-2023-25870 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Substance, 3d_stage or a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a not-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25871 er QVE-2023-25872 er QVE-2023-25872 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a victim for this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a repart of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25872 er er victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a repart of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25873 er er victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a victim file and provide average this vulnerability when parsing a crafted file, which			,			
affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current substance, 3d_stag er victim must open a malicious file. Adobe Substance 3D stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Substance, 3d_stage er Adobe Substance 3D stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Substance, 3d_stage substance, 3d_stage, 3d_	CVE-2023-25867		·	2023-03-27	7.8	High
result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a 2023-03-27 7.8 High Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this substance 3d_stag er must open a malicious file. QVE-2023-25869 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could result in arbitrary code execution in that a victim must open a malicious file. QVE-2023-25870 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25871 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25871 er Mode Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25872 er After Free vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. QVE-2023-25873 er After Free vulnerability when			· · · · · · · · · · · · · · · · · · ·			
substance_3d_stag er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Substance_3d_stag er Adobe Substa			· · · · · · · · · · · · · · · · · · ·			
victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Substance 3d_stag er must open a malicious file. QVE-2023-25869 er must open a malicious file. QVE-2023-25870 er must open a malicious file. QVE-2023-25871 er must open a malicious file. QVE-2023-25872 er must open a malicious file. QVE-2023-25873 er must open a malicious file. QVE-2023-25874 er must open a malicious file. QVE-2023-25874 er must open a malicious file. QVE-2023-25875 er must open a malicious file. QVE-2023-25876 er must open a malicious file. QVE-2023-25877 er must open a malicious file. QVE-2023-25878 er must open a malicious file. QVE-2023-25879 er must open a must open a must open						
Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25870 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a ma	CVF-2023-25868			2023-03-27	7.8	High
cyte-2023-25879 crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Cyte-2023-25870 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Cyte-2023-25871 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Cyte-2023-25871 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a volt-of-bounds requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an unt-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Cyte-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerabil	<u> </u>	C.		2023 03 27	7.0	6
allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. VE-2023-25870 Exploitation of this issue requires user interaction in that a victim must open a malicious file. VE-2023-25871 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. VE-2023-25871 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. VE-2023-25872 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and ea			affected by an out-of-bounds read vulnerability when parsing a			
adobe - substance_3d_stage er witherability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25870 er must open a malicious file. Adobe Substance_3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25871 er must open a malicious file. Adobe Substance_3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er en with the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) are affected by a Use After free vulnerability that could result in arbitrary code execution in the contex			·			
substance_3d_stag er Modoe_substance_3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Substance_3d_stag er Adobe_substance_3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Substance_3d_stag er CVE-2023-25871 er Adobe_substance_3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance_3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance_3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance_3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance_3D Stager versions 2.0.0 (and earlier) are affected by a heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Photos		adobo				
CVE-2023-25879 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25871 er Mobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user intera			·			
affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Desphased Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Ex	CVE-2023-25869			2023-03-27	7.8	High
adobe - substance_3d_stag			· · · · · · · · · · · · · · · · · · ·			
substance_3d_stag CVE-2023-25870 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25871 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er wich must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage to substance 3d stag vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in that a victim must open a malicious file. CVE-2023-25874 er victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitat						
CVE-2023-25870 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25871 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er vicin must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Mobbe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Photoshop versions 2.3.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.						
Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim arbitrary cod	CVE-2023-25870			2023-03-27	7.8	High
adobe - substance_3d_stag er			·			
substance_3d_stag er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25872 er CVE-2023-25872 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. 2023-03-27 7.8 High Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			affected by a Use After Free vulnerability that could result in			
CVE-2023-25871 er must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a must open a malicious file. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Substance_3d_stag user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er versions 2.0.0 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			•			
Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. 2023-03-27 7.8 High Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er CVE-2023-25874 er Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	C\/F_2022 25071		· ·	2022-02 27	70	⊔iah
affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	CVE-2U23-238/1	eı	'	2023-03-2/	1.6	ывп
result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			The state of the s			
CVE-2023-25872 er victim must open a malicious file. 2023-03-27 7.8 High Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. 2023-03-27 7.8 High CVE-2023-25873 er must open a malicious file. 2023-03-27 7.8 High Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. 2023-03-27 7.8 High Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. 2023-03-27 7.8 High			result in arbitrary code execution in the context of the current			
Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	0.45 - 5		·			
affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	CVE-2023-25872	er		2023-03-27	7.8	High
crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.						
allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25873 er Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			, , , , , , , , , , , , , , , , , , , ,			
adobe - substance_3d_stag er			·			
CVE-2023-25873 er must open a malicious file. 2023-03-27 7.8 High Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. 2023-03-27 7.8 High CVE-2023-25874 er Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			vulnerability to execute code in the context of the current user.			
Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	C) /F 2022 275		ļ ,	2022 02 2=	7.0	
affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE-2023-25874 er Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	CVE-2023-25873	er	'	2023-03-27	7.8	High
adobe - substance_3d_stag er victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			The state of the s			
substance_3d_stag er Victim must open a malicious file. Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a 1023-03-27 7.8 High Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a		adobe -	, , ,			
CVE-2023-25874 er victim must open a malicious file. 2023-03-27 7.8 High Adobe Photoshop versions 23.5.3 (and earlier) and 24.1.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			,			
earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	CVE-2023-25874			2023-03-27	7.8	High
result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a			· · · · · · · · · · · · · · · · · · ·			
adobe - multiple user. Exploitation of this issue requires user interaction in that a						
		adobe - multiple	,			
CVE-2023-25908 products victim must open a malicious file. 2023-03-27 7.8 High	CVE-2023-25908	•	·	2023-03-27	7.8	High

		Zoom Client for IT Admin macOS installers before version 5.13.5 contain a local privilege escalation vulnerability. A local low-			
		privileged user could exploit this vulnerability in an attack chain			
		during the installation process to escalate their privileges to			
CVE-2023-28596	zoom - meetings	privileges to root. A buffer overflow vulnerability was found in the Netfilter	2023-03-27	7.8	High
		subsystem in the Linux Kernel. This issue could allow the leakage			
	linux - multiple	of both stack and heap addresses, and potentially allow Local			
CVE-2023-0179	products	Privilege Escalation to the root user via arbitrary code execution.	2023-03-27	7.8	High
	huawai multinla	The InputMethod module has a vulnerability of			
CVE-2023-26547	huawei - multiple products	serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation.	2023-03-27	7.8	High
011 1010 100 17	p. ca.acts	Adobe Dimension versions 3.4.7 (and earlier) is affected by an		7.10	
		Improper Input Validation vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
CVE-2023-25879	adobe - dimension	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
<u> </u>	adose amiension	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2020 00 20	7.0	
		of-bounds write vulnerability that could result in arbitrary code			
		execution in the context of the current user. Exploitation of this			
CVE-2023-25880	adobe - dimension	issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
CVL-2023-23880	adobe - difficusion	Adobe Dimension versions 3.4.7 (and earlier) is affected by an	2023-03-28	7.8	riigii
		Improper Input Validation vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
CVE-2023-25881	adobe - dimension	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
CVL-2023-23881	adobe - difficusion	Adobe Dimension versions 3.4.7 (and earlier) is affected by a	2023-03-28	7.0	Iligii
		Heap-based Buffer Overflow vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
CVE-2023-25882	adobe - dimension	Exploitation of this issue requires user interaction in that a victim	2023-03-28	7.8	⊔iah
<u>CVE-2023-23882</u>	adobe - dimension	must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by a	2023-03-28	7.8	High
		Heap-based Buffer Overflow vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
0.45 0000 05000		Exploitation of this issue requires user interaction in that a victim			
CVE-2023-25883	adobe - dimension	must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-28	7.8	High
		of-bounds read vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute			
		code in the context of the current user. Exploitation of this issue			
CVE-2023-25884	adobe - dimension	requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by a			
		Heap-based Buffer Overflow vulnerability that could result in			
		arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim			
CVE-2023-25885	adobe - dimension	must open a malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue			
		requires user interaction in that a victim must open a malicious			
CVE-2023-25886	adobe - dimension	file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute			
		code in the context of the current user. Exploitation of this issue			
0/5 2022 25007	a dala a dia a dia a	requires user interaction in that a victim must open a malicious	2022 02 20	7.0	112.1.
CVE-2023-25887	adobe - dimension	file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-28	7.8	High
		of-bounds read vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute			
		code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious			
CVE-2023-25888	adobe - dimension	file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			U··
		of-bounds read vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue			
		requires user interaction in that a victim must open a malicious			
CVE-2023-25889	adobe - dimension	file. Adobe Dimension versions 3.4.7 (and earlier) is affected by a	2023-03-28	7.8	High

		arbitrary code execution in the context of the current user.			
		Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute			
		code in the context of the current user. Exploitation of this issue			
		requires user interaction in that a victim must open a malicious			
CVE-2023-25891	adobe - dimension	file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out- of-bounds read vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute			
		code in the context of the current user. Exploitation of this issue			
		requires user interaction in that a victim must open a malicious			
CVE-2023-25892	adobe - dimension	file. Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use	2023-03-28	7.8	High
		After Free vulnerability that could result in arbitrary code			
		execution in the context of the current user. Exploitation of this			
		issue requires user interaction in that a victim must open a			
CVE-2023-25893	adobe - dimension	malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use			
		After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this			
		issue requires user interaction in that a victim must open a			
CVE-2023-25894	adobe - dimension	malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by a			<u> </u>
		Heap-based Buffer Overflow vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
CVE 2022 2E90E	adobe - dimension	Exploitation of this issue requires user interaction in that a victim	2022 02 20	7.0	⊔iah
CVE-2023-25895	adobe - dimension	must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use	2023-03-28	7.8	High
		After Free vulnerability that could result in arbitrary code			
		execution in the context of the current user. Exploitation of this			
		issue requires user interaction in that a victim must open a			
CVE-2023-25896	adobe - dimension	malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by a			
		Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user.			
		Exploitation of this issue requires user interaction in that a victim			
CVE-2023-25897	adobe - dimension	must open a malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by a			
		Heap-based Buffer Overflow vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
CVE-2023-25898	adobe - dimension	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
<u> </u>	daobe differentiation	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use	2023 03 20	7.0	8
		After Free vulnerability that could result in arbitrary code			
		execution in the context of the current user. Exploitation of this			
		issue requires user interaction in that a victim must open a			
CVE-2023-25899	adobe - dimension	malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out- of-bounds read vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated memory			
		structure. An attacker could leverage this vulnerability to execute			
		code in the context of the current user. Exploitation of this issue			
		requires user interaction in that a victim must open a malicious			
CVE-2023-25900	adobe - dimension	file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an	2023-03-28	7.8	High
		Improper Input Validation vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
		Exploitation of this issue requires user interaction in that a victim			
CVE-2023-25901	adobe - dimension	must open a malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability when parsing a crafted file, which			
		could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute			
		code in the context of the current user. Exploitation of this issue			
		requires user interaction in that a victim must open a malicious			
CVE-2023-25902	adobe - dimension	file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an			
		Integer Overflow or Wraparound vulnerability that could result in			
		arbitrary code execution in the context of the current user.			
CVE-2023-25903	adobe - dimension	Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
CAT 7072-73202	adobe - diffiction	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-20	7.0	ıııgıı
		of-bounds read vulnerability when parsing a crafted file, which			
	i	could result in a read past the end of an allocated memory	2023-03-28	7.8	High

	<u></u>	,			
		structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out- of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this			
CVE-2023-25905	adobe - dimension	issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out- of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious			
CVE-2023-25906	adobe - dimension	file.	2023-03-28	7.8	High
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out- of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious	2022 02 20	7.0	ur. l
CVE-2023-25907	adobe - dimension	file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-28	7.8	High
CVE-2023-26327	adobe - dimension	of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
CVE 2022 2022	adalas de	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out- of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a	2022 02 22	7.0	10.1
CVE-2023-26328	adobe - dimension	malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-28	7.8	High
CVE-2023-26329	adobe - dimension	of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	2023-03-28	7.8	High
CVE-2023-26330	adobe - dimension	issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
CVE-2023-26331	adobe - dimension	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to	2023-03-28	7.8	High
CVE-2023-26332	adobe - dimension	bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-28	7.8	High
		of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious			
CVE-2023-26333	adobe - dimension	file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim	2023-03-28	7.8	High
CVE-2023-26334	adobe - dimension	must open a malicious file.	2023-03-28	7.8	High
CVE-2023-26335	adobe - dimension	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out- of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	2023-03-28	7.8	High
CVE-2023-26336	adobe - dimension	issue requires user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by a	2023-03-28	7.8	High
CVE-2023-26337	adobe - dimension	Stack-based Buffer Overflow vulnerability that could result in	2023-03-28	7.8	High

		arbitrary code execution in the context of the current user.			
		Exploitation of this issue requires user interaction in that a victim			
		must open a malicious file.			
		A vulnerability was found in the device-mapper-multipath. The			
		device-mapper-multipath allows local users to obtain root access,			
		exploited alone or in conjunction with CVE-2022-41973. Local users that are able to write to UNIX domain sockets can bypass			
		access controls and manipulate the multipath setup. This issue			
		occurs because an attacker can repeat a keyword, which is			
	redhat - multiple	mishandled when arithmetic ADD is used instead of bitwise OR.			
CVE-2022-3787	products	This could lead to local privilege escalation to root.	2023-03-29	7.8	High
		A double-free flaw was found in the Linux kernel's TUN/TAP device			
		driver functionality in how a user registers the device when the			
		register_netdevice function fails (NETDEV_REGISTER notifier). This			
CVE-2022-4744	linux - linux_kernel	flaw allows a local user to crash or potentially escalate their privileges on the system.	2023-03-30	7.8	High
<u>CVL-2022-4744</u>	iiiiux - iiiiux_keriiei	A flaw use after free in the Linux kernel Xircom 16-bit PCMCIA (PC-	2023-03-30	7.0	riigii
		card) Ethernet driver was found. A local user could use this flaw to			
		crash the system or potentially escalate their privileges on the			
CVE-2023-1670	linux - linux_kernel	system.	2023-03-30	7.8	High
	_	hci_conn_cleanup in net/bluetooth/hci_conn.c in the Linux kernel			
		through 6.2.9 has a use-after-free (observed in			
		hci_conn_hash_flush) because of calls to hci_dev_put and			
		hci_conn_put. There is a double free that may lead to privilege			
CVE-2023-28464	linux - linux_kernel	escalation.	2023-03-31	7.8	High
		An issue in the bridge2 component of MikroTik RouterOS v6.40.5			
CVE 2022 24004	mikrotik - routeros	allows attackers to cause a Denial of Service (DoS) via crafted	2023-03-27	7 5	⊔iah
CVE-2023-24094	mikrotik - routeros	packets. Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and	2023-03-27	7.5	High
		earlier) are affected by an XML Injection vulnerability that could			
		lead to arbitrary file system read. An unauthenticated attacker can			
		force the application to make arbitrary requests via injection of			
	adobe - multiple	arbitrary URLs. Exploitation of this issue does not require user			
CVE-2023-22247	products	interaction.	2023-03-27	7.5	High
		Zoom clients prior to 5.13.5 contain an improper trust boundary			
		implementation vulnerability. If a victim saves a local recording to			
		an SMB location and later opens it using a link from Zoom's web			
		portal, an attacker positioned on an adjacent network to the			
		victim client could set up a malicious SMB server to respond to			
	zoom multiple	client requests, causing the client to execute attacker controlled			
CVE-2023-28597	zoom - multiple products	executables. This could result in an attacker gaining access to a user's device and data, and remote code execution.	2023-03-27	7.5	High
CVL-2023-28337	products	The HwContacts module has a logic bypass vulnerability.	2023-03-27	7.5	riigii
	huawei - multiple	Successful exploitation of this vulnerability may affect			
CVE-2022-48346	products	confidentiality.	2023-03-27	7.5	High
	·	The MediaProvider module has a vulnerability in permission			
	huawei - multiple	verification. Successful exploitation of this vulnerability may affect			
CVE-2022-48347	products	confidentiality.	2023-03-27	7.5	High
		The HUAWEI Messaging app has a vulnerability of unauthorized			
	huawei - multiple	file access. Successful exploitation of this vulnerability may affect			
CVE-2022-48350	products	confidentiality.	2023-03-27	7.5	High
CVE 2022 402E1	huawei - multiple	The secure OS module has configuration defects. Successful	2022 02 27	7.5	ماء: ١١:
CVE-2022-48351	products huawei - multiple	exploitation of this vulnerability may affect availability. Some smartphones have data initialization issues. Successful	2023-03-27	7.5	High
CVE-2022-48352	products	exploitation of this vulnerability may cause a system panic.	2023-03-27	7.5	High
CVL 2022 +0332	products	The facial recognition module has a vulnerability in input	2023 03 27	7.5	111811
	huawei - multiple	parameter verification. Successful exploitation of this vulnerability			
CVE-2022-48356	products	may cause failed facial recognition.	2023-03-27	7.5	High
	·	Some products have the double fetch vulnerability. Successful			
	huawei - multiple	exploitation of this vulnerability may cause denial of service (DoS)			
CVE-2022-48357	products	attacks to the kernel.	2023-03-27	7.5	High
		The recovery mode for updates has a vulnerability that causes			
	huawei - multiple	arbitrary disk modification. Successful exploitation of this			
CVE-2022-48359	products	vulnerability may affect confidentiality.	2023-03-27	7.5	High
	haranat a terri	The facial recognition module has a vulnerability in file permission			
CVE 2022 402C0	huawei - multiple	control. Successful exploitation of this vulnerability may affect	2022 02 27	7 -	ما ما ۱
CVE-2022-48360	products	confidentiality. A bug affects the Linux kernel's ksmbd NTLMv2 authentication and	2023-03-27	7.5	High
CVE-2023-0210	linux - linux_kernel	is known to crash the OS immediately in Linux-based systems.	2023-03-27	7.5	High
<u> </u>	max max_kerner	Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25	2023 03 27	,.5	111811
		using "**" as a pattern in Spring Security configuration with the			
		mvcRequestMatcher creates a mismatch in pattern matching			
	vmware - multiple	between Spring Security and Spring MVC, and the potential for a			
CVE-2023-20860	products	security bypass.	2023-03-27	7.5	High
<u> </u>		The pgmng module has a vulnerability in			
		·			
CVE-2023-26548	huawei - multiple products	serialization/deserialization. Successful exploitation of this vulnerability may affect availability.	2023-03-27	7.5	High

	huawei - multiple	The SystemUI module has a vulnerability of repeated app restart due to improper parameters. Successful exploitation of this			
CVE-2023-26549	products	vulnerability may affect confidentiality.	2023-03-27	7.5	High
		This vulnerability allows remote attackers to read arbitrary files on			
		affected installations of Ivanti Avalanche 6.3.3.101. Although authentication is required to exploit this vulnerability, the existing			
		authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw			
		exists within the AgentTaskHandler class. The issue results from			
		the lack of proper validation of a user-supplied path prior to using			
		it in file operations. An attacker can leverage this vulnerability to			
CVE 2022 20002	i romti a ralamaha	disclose stored session cookies, leading to further compromise.	2022 02 20	7.5	I I i ada
CVE-2022-36982	ivanti - avalanche	Was ZDI-CAN-15967. The BatteryHealthActivity has a redirection vulnerability.	2023-03-29	7.5	High
	huawei - multiple	Successful exploitation of this vulnerability by a malicious app can			
CVE-2022-48358	products	cause service exceptions.	2023-03-27	7.4	High
		A slab-out-of-bound read problem was found in			
		brcmf_get_assoc_ies in			
		drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux Kernel. This issue could occur when assoc_info-			
		>req_len data is bigger than the size of the buffer, defined as			
CVE-2023-1380	linux - linux_kernel	WL_EXTRA_BUF_MAX, leading to a denial of service.	2023-03-27	7.1	High
	-	A use-after-free flaw was found in nfsd4_ssc_setup_dul in			
		fs/nfsd/nfs4proc.c in the NFS filesystem in the Linux Kernel. This			
	linux - multiple	issue could allow a local attacker to crash the system or it may		_	
CVE-2023-1652	products	lead to a kernel information leak problem.	2023-03-29	7.1	High
		A flaw was found in the Linux kernel. A use-after-free may be			
		triggered in asus_kbd_backlight_set when plugging/disconnecting in a malicious USB device, which advertises itself as an Asus			
		device. Similarly to the previous known CVE-2023-25012, but in			
		asus devices, the work_struct may be scheduled by the LED			
		controller while the device is disconnecting, triggering a use-after-			
		free on the struct asus_kbd_leds *led structure. A malicious USB			
0.45.0000	,	device may exploit the issue to cause memory corruption with	2025 5	<u> </u>	
CVE-2023-1079	linux - linux_kernel	controlled data.	2023-03-27	6.8	Medium
		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03			
		routers. Although authentication is required to exploit this			
		vulnerability, the existing authentication mechanism can be			
		bypassed. The specific flaw exists within the handling of			
		ConfigFileUpload requests to the web management portal. The			
		issue results from the lack of proper validation of a user-supplied			
	The transfer of	string before using it as a format specifier. An attacker can			
CVE-2022-43619	d-link - multiple products	leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16141.	2023-03-29	6.8	Medium
CVL-2022-43013	products	This vulnerability allows network-adjacent attackers to execute	2023-03-29	0.8	iviculuiii
		arbitrary code on affected installations of D-Link DIR-1935 1.03			
		routers. Although authentication is required to exploit this			
		vulnerability, the existing authentication mechanism can be			
		bypassed. The specific flaw exists within the handling of			
		SetWebFilterSetting requests to the web management portal. When parsing the WebFilterURLs element, the process does not			
		, -		ļ	
		properly validate a user-supplied string before using it to execute a 1			
	d-link - multiple	properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute			
CVE-2022-43623	d-link - multiple products	properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140.	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management	2023-03-29	6.8	Medium
CVE-2022-43623	•	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root.			Medium
CVE-2022-43623 CVE-2022-43624	products	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145.	2023-03-29	6.8	
	products d-link - multiple	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute			
	products d-link - multiple	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03			
	products d-link - multiple	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this			
	products d-link - multiple	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be			
	products d-link - multiple	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of			
	products d-link - multiple	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be			
	products d-link - multiple	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv4Settings requests to the web management			
	d-link - multiple products	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv4Settings requests to the web management portal. When parsing the NetMask element, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage			
CVE-2022-43624	d-link - multiple products	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv4Settings requests to the web management portal. When parsing the NetMask element, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-	2023-03-29	6.8	Medium
	d-link - multiple products	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv4Settings requests to the web management portal. When parsing the NetMask element, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16144.			Medium Medium
CVE-2022-43624	d-link - multiple products	system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16140. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv6Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv6List element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16145. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetStaticRouteIPv4Settings requests to the web management portal. When parsing the NetMask element, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-	2023-03-29	6.8	Medium

	Г	T			1
		vulnerability, the existing authentication mechanism can be			
		bypassed. The specific flaw exists within the handling of			
		SetIPv4FirewallSettings requests to the web management portal.			
		When parsing subelements within the IPv4FirewallRule element,			
		the process does not properly validate a user-supplied string			
		before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-			
		CAN-16146.			
		This vulnerability allows network-adjacent attackers to execute			
		arbitrary code on affected installations of D-Link DIR-1935 1.03			
		routers. Although authentication is required to exploit this			
		vulnerability, the existing authentication mechanism can be			
		bypassed. The specific flaw exists within the handling of			
		SetStaticRoutelPv4Settings requests to the web management			
		portal. When parsing subelements within the StaticRoutelPv4Data			
		element, the process does not properly validate a user-supplied			
		string before using it to execute a system call. An attacker can			
	d-link - multiple	leverage this vulnerability to execute code in the context of root.			
CVE-2022-43627	products	Was ZDI-CAN-16147.	2023-03-29	6.8	Medium
<u>CVL 2022 43027</u>	products	This vulnerability allows network-adjacent attackers to execute	2023 03 23	0.0	IVICUIUIII
		arbitrary code on affected installations of D-Link DIR-1935 1.03			
		routers. Although authentication is required to exploit this			
		vulnerability, the existing authentication mechanism can be			
		bypassed. The specific flaw exists within the handling of			
		SetIPv6FirewallSettings requests to the web management portal.			
		When parsing subelements within the IPv6FirewallRule element,			
		the process does not properly validate a user-supplied string			
		before using it to execute a system call. An attacker can leverage			
	d-link - multiple	this vulnerability to execute code in the context of root. Was ZDI-			
CVE-2022-43628	products	CAN-16148.	2023-03-29	6.8	Medium
2122322 10020	p. 04400	This vulnerability allows network-adjacent attackers to execute		3.0	caiaiii
		arbitrary code on affected installations of D-Link DIR-1935 1.03			
		routers. Although authentication is required to exploit this			
		vulnerability, the existing authentication mechanism can be			
		bypassed. The specific flaw exists within the handling of			
		SetSysEmailSettings requests to the web management portal.			
		When parsing subelements within the SetSysEmailSettings			
		element, the process does not properly validate a user-supplied			
		string before using it to execute a system call. An attacker can			
	d-link - multiple	leverage this vulnerability to execute code in the context of root.			
CVE_2022_42620	products	Was ZDI-CAN-16149.	2023-03-29	6.8	Medium
CVE-2022-43629					
CVL-2022-43029	•		2023 03 23	3.0	
<u>CVL-2022-43029</u>		This vulnerability allows network-adjacent attackers to execute	2020 00 23	3.0	
<u>CVL-2022-43029</u>		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03	2020 00 25	3.0	
<u>CVL-2022-43029</u>		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this	2020 00 23	5.0	
CVL-2022-43029		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be	2023 03 23	5.0	
<u>CVL-2022-43029</u>		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of	2023 03 23	5.0	
CVL-2022-43029		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal.	2020 00 23	3.0	
CVE-2022-43029		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element,	2023 03 23	5.5	
CVL-2022-43029		This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string	2023 03 23	5.5	
CVL-2022-43029	d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage	2020 00 20	5.5	
CVE-2022-43631	d-link - multiple products	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string	2023-03-29	6.8	
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151.			Medium
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151.			
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03			
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this			
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be			
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of			
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be			
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When			
	·	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does			
	products	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to			
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153.	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When	2023-03-29	6.8	Medium
CVE-2022-43631	products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly	2023-03-29	6.8	Medium
CVE-2022-43631	d-link - multiple products	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632	d-link - multiple products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute a system call. An attacker can leverage this vulnerability to execute a system call. An attacker can leverage this vulnerability to execute code in	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632	d-link - multiple products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16154.	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632	d-link - multiple products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16154. Insecure Win32 memory objects in Endpoint Windows Agents in	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632	d-link - multiple products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16154. Insecure Win32 memory objects in Endpoint Windows Agents in RSA NetWitness Platform before 12.2 allow local and admin	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632	d-link - multiple products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16154. Insecure Win32 memory objects in Endpoint Windows Agents in RSA NetWitness Platform before 12.2 allow local and admin Windows user accounts to modify the endpoint agent se	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632	d-link - multiple products d-link - multiple	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability, allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16154. Insecure Win32 memory objects in Endpoint Windows Agents in RSA NetWitness Platform before 12.2 allow local and admin Windows user accounts to modify the endpoint agent s	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632 CVE-2022-43633	d-link - multiple products d-link - multiple products	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute a system call. An attacker can leverage this vulnerability to execute a code in the context of root. Was ZDI-CAN-16154. Insecure Win32 memory objects in Endpoint Windows Agents in RSA NetWitness Platform before 12.2 all	2023-03-29	6.8	Medium
CVE-2022-43631 CVE-2022-43632 CVE-2022-43633	d-link - multiple products d-link - multiple products	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetVirtualServerSettings requests to the web management portal. When parsing subelements within the VirtualServerInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16151. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetQoSSettings requests to the web management portal. When parsing subelements within the QoSInfo element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16153. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DIR-1935 1.03 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of SetSysLogSettings requests to the web management portal. When parsing the IPAddress element, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16154. Insecure Win32 memory objects in Endpoint Windows Agents in RSA NetWitness Platform before 12.2 allow local and admin Windows user accounts to modify the endpoint agent se	2023-03-29	6.8	Medium

	T			T	T
		USB device. This flaw allows a local user to crash or potentially			
		escalate their privileges on the system. TensorFlow is an Open Source Machine Learning Framework. In			
		versions prior to 2.11.1 a malicious invalid input crashes a			
		tensorflow model (Check Failed) and can be used to trigger a			
		denial of service attack. A proof of concept can be constructed			
		with the `Convolution3DTranspose` function. This			
		Convolution3DTranspose layer is a very common API in modern			
		neural networks. The ML models containing such vulnerable			
		components could be deployed in ML applications or as cloud			
		services. This failure could be potentially used to trigger a denial of service attack on ML cloud services. An attacker must have			
		privilege to provide input to a `Convolution3DTranspose` call. This			
		issue has been patched and users are advised to upgrade to			
		version 2.11.1. There are no known workarounds for this			
CVE-2023-25661	google - tensorflow	vulnerability.	2023-03-27	6.5	Mediun
		The Bluetooth module has an authentication bypass vulnerability			
	huawei - multiple	in the pairing process. Successful exploitation of this vulnerability			
CVE-2022-48291	products	may affect confidentiality.	2023-03-27	6.5	Mediun
	huawei - multiple	The Bluetooth module has a heap out-of-bounds write			
CVE-2022-48354	products	vulnerability. Successful exploitation of this vulnerability can cause the Bluetooth process to crash.	2023-03-27	6.5	Mediun
CVL 2022 40334	products	The Bluetooth module has a heap out-of-bounds read	2023 03 27	0.5	ivicalan
	huawei - multiple	vulnerability. Successful exploitation of this vulnerability can cause			
CVE-2022-48355	products	the Bluetooth process to crash.	2023-03-27	6.5	Mediun
		This vulnerability allows network-adjacent attackers to disclose			
		sensitive information on affected installations of TP-Link TL-			
		WR940N 3.20.1 Build 200316 Rel.34392n (5553) routers.			
		Authentication is not required to exploit this vulnerability. The			
		specific flaw exists within the httpd service, which listens on TCP			
		port 80 by default. The issue results from the lack of proper access control. An attacker can leverage this vulnerability to disclose			
	tp-link - tl-	stored credentials, leading to further compromise. Was ZDI-CAN-			
CVE-2022-24972	wr940n firmware	13911.	2023-03-28	6.5	Mediun
<u> </u>		This vulnerability allows network-adjacent attackers to disclose		0.0	
		sensitive information on affected installations of TP-Link TL-			
		WR940N 6_211111 3.20.1(US) routers. Authentication is not			
		required to exploit this vulnerability. The specific flaw exists within			
		the httpd service, which listens on TCP port 80 by default. The			
		issue results from the incorrect implementation of the			
	to link th	authentication algorithm. An attacker can leverage this			
CVE-2022-43635	tp-link - tl- wr940n_firmware	vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-17332.	2023-03-29	6.5	Medium
CVL 2022 +3033	wi540ii_iiiiiwaic	Improper Neutralization of Special Elements used in an SQL	2023 03 23	0.5	ivicaian
		Command ('SQL Injection') vulnerability in Apache Software			
		Foundation apache fineract. Authorized users may be able to			
		exploit this for limited impact on components. This issue affects			
CVE-2023-25197	apache - fineract	apache fineract: from 1.4 through 1.8.2.	2023-03-28	6.3	Mediun
		A flaw was found in the Keycloak Node.js Adapter. This flaw allows			
CVE 2022 2227	redhat - multiple	an attacker to benefit from an Open Redirect vulnerability in the	2022 02 27	6.1	N A maliana
CVE-2022-2237	products	checkSso function.	2023-03-27	6.1	Mediun
		A memory leak flaw was found in the Linux kernel's Stream Control Transmission Protocol. This issue may occur when a user starts a			
		malicious networking service and someone connects to this			
		service. This could allow a local user to starve resources, causing a			
CVE-2023-1074	linux - linux_kernel	denial of service.	2023-03-27	5.5	Mediun
	_	A flaw was found in the Linux Kernel. The tun/tap sockets have			
		their socket UID hardcoded to 0 due to a type confusion in their			
		initialization function. While it will be often correct, as tuntap			
		devices require CAP_NET_ADMIN, it may not always be the case,			
		e.g., a non-root user only having that capability. This would make			
CVE-2023-1076	linux - linux_kernel	tun/tap sockets being incorrectly treated in filtering/routing decisions, possibly bypassing network filters.	2023-03-27	5.5	Mediur
CVL-2023-10/0	miux - miux_kernel	Adobe Substance 3D Stager versions 2.0.0 (and earlier) are	2023-03-27	3.5	ivieulufi
		· · · · · · · · · · · · · · · · · · ·			
		l affected by an out-of-bounds read vulnerability that could lead to			
		affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this			
	adobe -				
	adobe - substance_3d_stag	disclosure of sensitive memory. An attacker could leverage this			
CVE-2023-25875		disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-27	5.5	Mediun
CVE-2023-25875	substance_3d_stag	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are	2023-03-27	5.5	Mediun
CVE-2023-25875	substance_3d_stag	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to	2023-03-27	5.5	Mediun
CVE-2023-25875	substance_3d_stag er	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this	2023-03-27	5.5	Mediun
CVE-2023-25875	substance_3d_stag er adobe -	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of	2023-03-27	5.5	Mediun
	substance_3d_stag er adobe - substance_3d_stag	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a			
CVE-2023-25875 CVE-2023-25876	substance_3d_stag er adobe -	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-27	5.5	
	substance_3d_stag er adobe - substance_3d_stag	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are			
	substance_3d_stag er adobe - substance_3d_stag er	disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Substance 3D Stager versions 2.0.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			Medium Medium

		this issue requires user interaction in that a victim must open a malicious file.			
		Adobe Substance 3D Stager versions 2.0.0 (and earlier) are			
		affected by an out-of-bounds read vulnerability that could lead to			
		disclosure of sensitive memory. An attacker could leverage this			
	adobe -	vulnerability to bypass mitigations such as ASLR. Exploitation of			
	substance_3d_stag	this issue requires user interaction in that a victim must open a			
CVE-2023-25878	er	malicious file.	2023-03-27	5.5	Medium
		A flaw that boot CPU could be vulnerable for the speculative			
		execution behavior kind of attacks in the Linux kernel X86 CPU			
		Power management options functionality was found in the way			
		user resuming CPU from suspend-to-RAM. A local user could use			
		this flaw to potentially get unauthorized access to some memory			
		of the CPU similar to the speculative execution behavior kind of			
CVE-2023-1637	linux - linux_kernel	attacks.	2023-03-27	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
0.45 0000 0000		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26338	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
CVE 2022 20220		bypass mitigations such as ASLR. Exploitation of this issue requires	2022 02 20		NA o divuso
CVE-2023-26339	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26340	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
<u>CVE 2023 203 10</u>	adobe difficilision	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023 03 20	3.3	ivicaiaiii
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26341	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26342	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26343	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an			
		Access of Uninitialized Pointer vulnerability that could lead to			
		disclosure of sensitive memory. An attacker could leverage this			
		vulnerability to bypass mitigations such as ASLR. Exploitation of			
0.45 0000 00044		this issue requires user interaction in that a victim must open a			
CVE-2023-26344	adobe - dimension	malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
CVE-2023-26345	adobe - dimension	bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
CVE-2025-20545	adobe - diffictioni	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-20	ر.ر	ivicululii
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26346	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	1_3 00 20		
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26348	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by a Use			
		After Free vulnerability that could lead to disclosure of sensitive			
		memory. An attacker could leverage this vulnerability to bypass			
		mitigations such as ASLR. Exploitation of this issue requires user			
CVE-2023-26349	adobe - dimension	interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		Trade Emicrosoft Versions St. 117 (and earlier) is affected by an out			
		of-bounds read vulnerability that could lead to disclosure of			
		· · · · · · · · · · · · · · · · · · ·			
		of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26350	adobe - dimension	of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
CVE-2023-26350	adobe - dimension	of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-28	5.5	Medium
CVE-2023-26350 CVE-2023-26351	adobe - dimension adobe - dimension	of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	5.5 5.5	Medium Medium

	T				T
		bypass mitigations such as ASLR. Exploitation of this issue requires			
		user interaction in that a victim must open a malicious file.			
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26352	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
CVE-2023-20332	adobe - difficision	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-26	٥.٥	Medium
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26353	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
CVE-2023-20333	adobe - difficilision	Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-	2023-03-26	3.3	Medium
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
CVE-2023-26354	adobe - dimension	bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
CVE-2023-20334	adobe - difficilsion	·	2023-03-26	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26355	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Adobe Dimension versions 3.4.7 (and earlier) is affected by an out-			
		of-bounds read vulnerability that could lead to disclosure of			
		sensitive memory. An attacker could leverage this vulnerability to			
		bypass mitigations such as ASLR. Exploitation of this issue requires			
CVE-2023-26356	adobe - dimension	user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
		Insertion of Sensitive Information into log file vulnerability in			
		NGINX Agent. NGINX Agent version 2.0 before 2.23.3 inserts			
		sensitive information into a log file. An authenticated attacker with			
		local access to read agent log files may gain access to private keys.			
		This issue is only exposed when the non-default trace level logging			
		is enabled. Note: NGINX Agent is included with NGINX Instance			
	f5 - multiple	Manager and used in conjunction with NGINX API Connectivity			
CVE-2023-1550	products	Manager, and NGINX Management Suite Security Monitoring.	2023-03-29	5.5	Medium
	,	Privilege escalation via stored XSS using the file upload service to			
		upload malicious content. The issue can be exploited only by			
		authenticated users which can create directory name to inject			
CVE-2023-28158	apache - archiva	some XSS content and gain some privileges such admin user.	2023-03-29	5.4	Medium
	·	A flaw was found in Keycloak in the execute-actions-email			
		endpoint. This issue allows arbitrary HTML to be injected into			
	redhat - multiple	emails sent to Keycloak users and can be misused to perform			
CVE-2022-1274	products	phishing or other attacks against users.	2023-03-29	5.4	Medium
<u>CVL 2022 1274</u>	products	A blind XML External Entity (XXE) vulnerability exists in the Add	2023 03 23	J. -	ivicaiaiii
		UCS Device functionality of ManageEngine OpManager 12.6.168. A			
	zohocorp - multiple	specially crafted XML file can lead to SSRF. An attacker can serve a			
CVE-2022-43473	products	malicious XML payload to trigger this vulnerability.	2023-03-30	5.4	Medium
VE-2022-43473	products	· · · · · · · · · · · · · · · · · · ·	2023-03-30	3.4	Medium
		In the Linux kernel through 6.2.8, net/bluetooth/hci_sync.c allows			
CVE 2022 20066	linus linus kornol	out-of-bounds access because amp_init1[] and amp_init2[] are	2022 02 27	гэ	Madium
CVE-2023-28866	linux - linux_kernel	supposed to have an intentionally invalid element, but do not.	2023-03-27	5.3	Medium
		Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and			
		earlier) are affected by an Improper Access Control vulnerability			
		that could result in a Security feature bypass. An attacker could			
		leverage this vulnerability to impact the availability of a user's			
	adobe - multiple	minor feature. Exploitation of this issue does not require user			
CVE-2023-22250	products	interaction.	2023-03-27	5.3	Medium
		The Always On Display (AOD) has a path traversal vulnerability in			
	huawei - multiple	theme files. Successful exploitation of this vulnerability may cause			
CVE-2022-48361	products	a failure in reading AOD theme resources.	2023-03-27	5.3	Medium
		Applications that use a non-default option when verifying			
		certificates may be vulnerable to an attack from a malicious CA to			
		circumvent certain checks. Invalid certificate policies in leaf			
		certificates are silently ignored by OpenSSL and other certificate			
		policy checks are skipped for that certificate. A malicious CA could			
		use this to deliberately assert invalid certificate policies in order to			
		circumvent policy checking on the certificate altogether. Policy			
		processing is disabled by default but can be enabled by passing the			
	openssl - multiple	`-policy' argument to the command line utilities or by calling the			
CVE-2023-0465	products	`X509_VERIFY_PARAM_set1_policies()' function.	2023-03-28	5.3	Medium
OVE 2023-0403	ρισαάστο	The function X509_VERIFY_PARAM_add0_policy() is documented	2023 03-20	ر. ر	iviculalii
		to implicitly enable the certificate policy check when doing			
		, , ,			
		certificate verification. However the implementation of the			
		function does not enable the check which allows certificates with			
		invalid or incorrect policies to pass the certificate verification. As			
		suddenly enabling the policy check could break existing			
	Ĺ	deployments it was decided to keep the existing behavior of the			
		VEGO VEDIEV BARANA LIG. 11 0.6			
		X509_VERIFY_PARAM_add0_policy() function. Instead the			
CVE-2023-0466	openssl - multiple products	X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or	2023-03-28	5.3	Medium

		explicitly enable the policy check by calling			
		X509_VERIFY_PARAM_set_flags() with the			
		X509_V_FLAG_POLICY_CHECK flag argument. Certificate policy			
		checks are disabled by default in OpenSSL and are not commonly			
		used by applications.			
		Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and			
		earlier) are affected by a stored Cross-Site Scripting (XSS)			
		vulnerability that could be abused by a high-privileged attacker to			
	adaha multinla	inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they			
CVE-2023-22249	adobe - multiple products	browse to the page containing the vulnerable field.	2023-03-27	4.8	Medium
CVL-2023-22243	products	This vulnerability allows local attackers to disclose sensitive	2023-03-27	4.0	Wiediaiii
		information on affected installations of the Linux Kernel 6.0-rc2.			
		An attacker must first obtain the ability to execute high-privileged			
		code on the target system in order to exploit this vulnerability. The			
		specific flaw exists within the nft_osf_eval function. The issue			
		results from the lack of proper initialization of memory prior to			
		accessing it. An attacker can leverage this in conjunction with			
		other vulnerabilities to execute arbitrary code in the context of the			
CVE-2022-42432	linux - linux_kernel	kernel. Was ZDI-CAN-18540.	2023-03-29	4.4	Medium
		Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and			
	adobo multipla	earlier) are affected by an Incorrect Authorization vulnerability. A			
CVE-2023-22251	adobe - multiple products	low-privileged authenticated attacker could leverage this vulnerability to achieve minor information disclosure.	2023-03-27	4.3	Medium
CAT TOTO-TTTT	products	Improper Neutralization of Special Elements used in an SQL	2023-03-27	٠,٠	IVICUIUIII
		Command ('SQL Injection') vulnerability in Apache Software			
		Foundation Apache Fineract. Authorized users may be able to			
		change or add data in certain components. This issue affects			
CVE-2023-25196	apache - fineract	Apache Fineract: from 1.4 through 1.8.2.	2023-03-28	4.3	Medium
		A vulnerability have been reported to affect multiple QNAP			
		operating systems. If exploited, the vulnerability allow remote			
		authenticated users to get secret values. The vulnerabilities affect			
		the following QNAP operating systems: QTS, QuTS hero,			
		QuTScloud, QVP (QVR Pro appliances) We have already fixed the			
	anan multinla	vulnerabilities in the following operating system versions: QTS 5.0.1.2346 build 20230322 and later QuTS hero h5.0.1.2348 build			
CVE-2022-27597	qnap - multiple products	20230324 and later	2023-03-29	4.3	Medium
CVL-2022-27331	products	A vulnerability have been reported to affect multiple QNAP	2023-03-23	4.5	Wiediaiii
		operating systems. If exploited, the vulnerability allow remote			
		authenticated users to get secret values. The vulnerabilities affect			
		the following QNAP operating systems: QTS, QuTS hero,			
		QuTScloud, QVP (QVR Pro appliances) We have already fixed the			
		vulnerabilities in the following operating system versions: QTS			
	qnap - multiple	5.0.1.2346 build 20230322 and later QuTS hero h5.0.1.2348 build			
CVE-2022-27598	products	20230324 and later	2023-03-29	4.3	Medium
		This vulnerability allows local attackers to execute arbitrary code			
		on affected installations of Samsung Galaxy S21 prior to 4.5.40.5			
		phones. An attacker must first obtain the ability to execute low- privileged code on the target system in order to exploit this			
		vulnerability. The specific flaw exists within the handling of			
		redirections. An attacker can force a redirection to a site that			
		serves malicious content. An attacker can leverage this in			
	samsung -	conjunction with other vulnerabilities to escalate privileges and			
	galaxy_s21_firmwa	execute arbitrary code in the context of the current user. Was ZDI-			
CVE-2022-1230	re	CAN-15918.	2023-03-28	3.9	Low
		A flaw was found in the Linux Kernel. The tls_is_tx_ready()			
		incorrectly checks for list emptiness, potentially accessing a type			
C) /F 2022 4677	Barrer Br. 1	confused entry to the list_head, leaking the last byte of the	2022 22 27	2.2	
CVE-2023-1075	linux - linux_kernel	confused field that overlaps with rec->tx_ready.	2023-03-27	3.3	Low
		A flaw was found in the Linux kernel's implementation of RDMA over infiniband. An attacker with a privileged local account can			
		LOVEL DUDDINADO, AD ATTACKEL WITH A DITIVILEGED INCAL ACCOUNT CAN			1
		, ·			
		leak kernel stack information when issuing commands to the			
	linux - multiple	, ·			

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's وإذ تبقى .NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.