الهيئة الوطنية
للأمن السيبراني
Nat onal Cybersecurity Authority

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 26th of March to 1st of April. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following 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 السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢٦ مارس إلى ١ أبريل. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـCVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2022-48353	huawei - multiple products	Some smartphones have configuration issues. Successful exploitation of this vulnerability may cause kernel privilege escalation, which results in system service exceptions.	2023-03-27	9.8	Critical
CVE-2023-28326	apache - openmeetings	Vendor: The Apache Software Foundation Versions Affected: Apache OpenMeetings from 2.0.0 before 7.0.0 Description: Attacker can elevate their privileges in any room	2023-03-28	9.8	Critical
CVE-2022-36972	ivanti - avalanche	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 bypass authentication on the system. Was ZDI-CAN-15328.	2023-03-29	9.8	Critical
CVE-2022-36974	ivanti - avalanche	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 the service account. Was ZDI-CAN-15330.	2023-03-29	9.8	Critical
CVE-2022-36975	ivanti - avalanche	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 bypass authentication on the system. Was ZDI-CAN-15332.	2023-03-29	9.8	Critical
CVE-2022-36976	ivanti - avalanche	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 bypass authentication on the system. Was ZDI-CAN-15333.	2023-03-29	9.8	Critical
CVE-2022-36977	ivanti - avalanche	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 data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-15449.	2023-03-29	9.8	Critical
CVE-2022-36978	ivanti - avalanche	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 Notification Server service. The issue results from the lack of proper validation of user-supplied data,	2023-03-29	9.8	Critical

		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.			
CVE-2022-36979	ivanti - avalanche	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 AvalancheDaoSupport class. A crafted request can trigger execution of SQL queries composed from a user-supplied string. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15493.	2023-03-29	9.8	Critical
CVE-2022-36981	ivanti - avalanche	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, the existing authentication mechanism can be bypassed. The specific flaw exists within the DeviceLogResource 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 execute code in the context of the service account. Was ZDI-CAN-15966.	2023-03-29	9.8	Critical
CVE-2022-36983	ivanti - avalanche	This vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche 6.3.3.101. 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 authentication on the system. Was ZDI-CAN-15919.	2023-03-29	9.8	Critical
CVE-2022-48348	huawei - multiple products	The MediaProvider module has a vulnerability of unauthorized data read. Successful exploitation of this vulnerability may affect confidentiality and integrity.	2023-03-27	9.1	Critical
CVE-2022-48349	huawei - multiple products	The control component has a spoofing vulnerability. Successful exploitation of this vulnerability may affect confidentiality and availability.	2023-03-27	9.1	Critical
CVE-2023-27296	apache - inlong	Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache InLong. It could be triggered by authenticated users of InLong, you could refer to [1] to know more about this vulnerability. This issue affects Apache InLong: from 1.1.0 through 1.5.0. Users are advised to upgrade to Apache InLong's latest version or cherry-pick [2] to solve it. [1] 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 https://github.com/apache/inlong/pull/7422	2023-03-27	8.8	High
CVE-2022-24352	tp-link - ac1750_firmware	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link AC1750 prior to 211210 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB.ko kernel 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 vulnerability to execute code in the context of root. Was ZDI-CAN-15773.	2023-03-28	8.8	High
CVE-2022-24353	tp-link - ac1750_firmware	This vulnerability allows network-adjacent attackers to execute 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 vulnerability to execute code in the context of the root user. Was ZDI-CAN-15769.	2023-03-28	8.8	High
CVE-2023-23355	qnap - multiple products	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 20230322 and later QuTS hero h5.0.1.2348 build 20230324 and later	2023-03-29	8.8	High
CVE-2022-27641	netgear - d7800_firmware	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 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

CVE-2022-27642	netgear - cax80_firmware	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 conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-15854.	2023-03-29	8.8	High
CVE-2022-27643	netgear - r6400_firmware	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 vulnerability to execute code in the context of root. Was ZDI-CAN-15692.	2023-03-29	8.8	High
CVE-2022-27644	netgear - r6400_firmware	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 presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-15797.	2023-03-29	8.8	High
CVE-2022-27645	netgear - lax20_firmware	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 readycloud_control.cgi. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15762.	2023-03-29	8.8	High
CVE-2022-27646	netgear - r6400_firmware	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 vulnerability to execute code in the context of root. Was ZDI-CAN-15879.	2023-03-29	8.8	High
CVE-2022-36971	ivanti - avalanche	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 the service account. Was ZDI-CAN-15301.	2023-03-29	8.8	High
CVE-2022-36973	ivanti - avalanche	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. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-15329.	2023-03-29	8.8	High
CVE-2022-43620	d-link - multiple products	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 authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-16142.	2023-03-29	8.8	High
CVE-2022-43621	d-link - multiple products	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 an incorrectly implemented comparison. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-16152.	2023-03-29	8.8	High
CVE-2022-43622	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. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of Login requests to the web management portal. When parsing the HNAP_AUTH header,	2023-03-29	8.8	High

		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.			
CVE-2022-43630	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. 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 attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16150.	2023-03-29	8.8	High
CVE-2022-43636	tp-link - tl-wr940n_firmware	This vulnerability allows network-adjacent attackers to bypass 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 vulnerability to bypass authentication on the system. Was ZDI-CAN-18334.	2023-03-29	8.8	High
CVE-2023-25195	apache - fineract	Server-Side Request Forgery (SSRF) vulnerability in Apache 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 Fineract: from 1.4 through 1.8.3.	2023-03-28	8.1	High
CVE-2022-36980	ivanti - avalanche	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 bypass authentication on the system. Was ZDI-CAN-15528.	2023-03-29	8.1	High
CVE-2022-0650	tp-link - tl-wr940n_firmware	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 buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13993.	2023-03-28	8	High
CVE-2022-24973	tp-link - tl-wr940n_firmware	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 buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13992.	2023-03-28	8	High
CVE-2022-27647	netgear - cax80_firmware	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 vulnerability to execute code in the context of root. Was ZDI-CAN-15874.	2023-03-29	8	High
CVE-2022-42433	tp-link - tl-wr841_firmware	This vulnerability allows network-adjacent attackers to execute 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 system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-17356.	2023-03-29	8	High
CVE-2023-1077	linux - linux_kernel	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 sched_rt_entity,causing memory corruption.	2023-03-27	7.8	High

CVE-2023-1078	linux - linux_kernel	A flaw was found in the Linux Kernel in RDS (Reliable Datagram Sockets) protocol. The rds_rm_zerocopy_callback() uses list_entry() on the head of a list causing a type confusion. Local user can trigger this with rds_message_put(). Type confusion leads to `struct rds_msg_zcopy_info *info` actually points to something else that is potentially controlled by local user. It is known how to trigger this, which causes an out of bounds access, and a lock corruption.	2023-03-27	7.8	High
CVE-2023-25863	adobe - substance_3d_stager	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-2023-25864	adobe - substance_3d_stager	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-2023-25865	adobe - substance_3d_stager	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.	2023-03-27	7.8	High
CVE-2023-25866	adobe - substance_3d_stager	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.	2023-03-27	7.8	High
CVE-2023-25867	adobe - substance_3d_stager	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.	2023-03-27	7.8	High
CVE-2023-25868	adobe - substance_3d_stager	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-2023-25869	adobe - substance_3d_stager	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-2023-25870	adobe - substance_3d_stager	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.	2023-03-27	7.8	High
CVE-2023-25871	adobe - substance_3d_stager	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.	2023-03-27	7.8	High
CVE-2023-25872	adobe - substance_3d_stager	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-2023-25873	adobe - substance_3d_stager	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-2023-25874	adobe - substance_3d_stager	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-2023-25908	adobe - multiple products	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

CVE-2023-28596	zoom - meetings	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 privileges to root.	2023-03-27	7.8	High
CVE-2023-0179	linux - multiple products	A buffer overflow vulnerability was found in the Netfilter subsystem in the Linux Kernel. This issue could allow the leakage of both stack and heap addresses, and potentially allow Local Privilege Escalation to the root user via arbitrary code execution.	2023-03-27	7.8	High
CVE-2023-26547	huawei - multiple products	The InputMethod module has a vulnerability of serialization/deserialization mismatch. Successful exploitation of this vulnerability may cause privilege escalation.	2023-03-27	7.8	High
CVE-2023-25879	adobe - dimension	Adobe Dimension versions 3.4.7 (and earlier) is 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.	2023-03-28	7.8	High
CVE-2023-25880	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-25881	adobe - dimension	Adobe Dimension versions 3.4.7 (and earlier) is 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.	2023-03-28	7.8	High
CVE-2023-25882	adobe - dimension	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 must open a malicious file.	2023-03-28	7.8	High
CVE-2023-25883	adobe - dimension	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 must open a malicious file.	2023-03-28	7.8	High
CVE-2023-25884	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.	2023-03-28	7.8	High
CVE-2023-25885	adobe - dimension	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 must open a malicious file.	2023-03-28	7.8	High
CVE-2023-25886	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.	2023-03-28	7.8	High
CVE-2023-25887	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.	2023-03-28	7.8	High
CVE-2023-25888	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.	2023-03-28	7.8	High
CVE-2023-25889	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.	2023-03-28	7.8	High
CVE-2023-25890	adobe - dimension	Adobe Dimension versions 3.4.7 (and earlier) is affected by a Heap-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.			
CVE-2023-25891	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.	2023-03-28	7.8	High
CVE-2023-25892	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.	2023-03-28	7.8	High
CVE-2023-25893	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-25894	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-25895	adobe - dimension	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 must open a malicious file.	2023-03-28	7.8	High
CVE-2023-25896	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-25897	adobe - dimension	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 must open a malicious file.	2023-03-28	7.8	High
CVE-2023-25898	adobe - dimension	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 must open a malicious file.	2023-03-28	7.8	High
CVE-2023-25899	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-25900	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.	2023-03-28	7.8	High
CVE-2023-25901	adobe - dimension	Adobe Dimension versions 3.4.7 (and earlier) is 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.	2023-03-28	7.8	High
CVE-2023-25902	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.	2023-03-28	7.8	High
CVE-2023-25903	adobe - dimension	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. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	7.8	High
CVE-2023-25904	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	2023-03-28	7.8	High

		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-2023-25905	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-25906	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.	2023-03-28	7.8	High
CVE-2023-25907	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.	2023-03-28	7.8	High
CVE-2023-26327	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.	2023-03-28	7.8	High
CVE-2023-26328	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-26329	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.	2023-03-28	7.8	High
CVE-2023-26330	adobe - dimension	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 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.	2023-03-28	7.8	High
CVE-2023-26332	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.	2023-03-28	7.8	High
CVE-2023-26333	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.	2023-03-28	7.8	High
CVE-2023-26334	adobe - dimension	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 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.	2023-03-28	7.8	High
CVE-2023-26336	adobe - dimension	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 malicious file.	2023-03-28	7.8	High
CVE-2023-26337	adobe - dimension	Adobe Dimension versions 3.4.7 (and earlier) is affected by a 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.			
CVE-2022-3787	redhat - multiple products	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 mishandled when arithmetic ADD is used instead of bitwise OR. This could lead to local privilege escalation to root.	2023-03-29	7.8	High
CVE-2022-4744	linux - linux_kernel	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 flaw allows a local user to crash or potentially escalate their privileges on the system.	2023-03-30	7.8	High
CVE-2023-1670	linux - linux_kernel	A flaw use after free in the Linux kernel Xircom 16-bit PCMCIA (PC-card) Ethernet driver was found.A local user could use this flaw to crash the system or potentially escalate their privileges on the system.	2023-03-30	7.8	High
CVE-2023-28464	linux - linux_kernel	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 escalation.	2023-03-31	7.8	High
CVE-2023-24094	mikrotik - routeros	An issue in the bridge2 component of MikroTik RouterOS v6.40.5 allows attackers to cause a Denial of Service (DoS) via crafted packets.	2023-03-27	7.5	High
CVE-2023-22247	adobe - multiple products	Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and 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 arbitrary URLs. Exploitation of this issue does not require user interaction.	2023-03-27	7.5	High
CVE-2023-28597	zoom - multiple products	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 client requests, causing the client to execute attacker controlled 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
CVE-2022-48346	huawei - multiple products	The HwContacts module has a logic bypass vulnerability. Successful exploitation of this vulnerability may affect confidentiality.	2023-03-27	7.5	High
CVE-2022-48347	huawei - multiple products	The MediaProvider module has a vulnerability in permission verification. Successful exploitation of this vulnerability may affect confidentiality.	2023-03-27	7.5	High
CVE-2022-48350	huawei - multiple products	The HUAWEI Messaging app has a vulnerability of unauthorized file access. Successful exploitation of this vulnerability may affect confidentiality.	2023-03-27	7.5	High
CVE-2022-48351	huawei - multiple products	The secure OS module has configuration defects. Successful exploitation of this vulnerability may affect availability.	2023-03-27	7.5	High
CVE-2022-48352	huawei - multiple products	Some smartphones have data initialization issues. Successful exploitation of this vulnerability may cause a system panic.	2023-03-27	7.5	High
CVE-2022-48356	huawei - multiple products	The facial recognition module has a vulnerability in input parameter verification. Successful exploitation of this vulnerability may cause failed facial recognition.	2023-03-27	7.5	High
CVE-2022-48357	huawei - multiple products	Some products have the double fetch vulnerability. Successful exploitation of this vulnerability may cause denial of service (DoS) attacks to the kernel.	2023-03-27	7.5	High
CVE-2022-48359	huawei - multiple products	The recovery mode for updates has a vulnerability that causes arbitrary disk modification. Successful exploitation of this vulnerability may affect confidentiality.	2023-03-27	7.5	High
CVE-2022-48360	huawei - multiple products	The facial recognition module has a vulnerability in file permission control. Successful exploitation of this vulnerability may affect confidentiality.	2023-03-27	7.5	High
CVE-2023-0210	linux - linux_kernel	A bug affects the Linux kernel's ksmbd NTLMv2 authentication and is known to crash the OS immediately in Linux-based systems.	2023-03-27	7.5	High
CVE-2023-20860	vmware - multiple products	Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and the potential for a security bypass.	2023-03-27	7.5	High
CVE-2023-26548	huawei - multiple products	The pgmng module has a vulnerability in serialization/deserialization. Successful exploitation of this vulnerability may affect availability.	2023-03-27	7.5	High

CVE-2023-26549	huawei - multiple products	The SystemUI module has a vulnerability of repeated app restart due to improper parameters. Successful exploitation of this vulnerability may affect confidentiality.	2023-03-27	7.5	High
CVE-2022-36982	ivanti - avalanche	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 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 disclose stored session cookies, leading to further compromise. Was ZDI-CAN-15967.	2023-03-29	7.5	High
CVE-2022-48358	huawei - multiple products	The BatteryHealthActivity has a redirection vulnerability. Successful exploitation of this vulnerability by a malicious app can cause service exceptions.	2023-03-27	7.4	High
CVE-2023-1380	linux - linux_kernel	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 WL_EXTRA_BUF_MAX, leading to a denial of service.	2023-03-27	7.1	High
CVE-2023-1652	linux - multiple products	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 issue could allow a local attacker to crash the system or it may lead to a kernel information leak problem.	2023-03-29	7.1	High
CVE-2023-1079	linux - linux_kernel	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 device may exploit the issue to cause memory corruption with controlled data.	2023-03-27	6.8	Medium
CVE-2022-43619	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 ConfigFileUpload requests to the web management portal. The issue results from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16141.	2023-03-29	6.8	Medium
CVE-2022-43623	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 SetWebFilterSetting requests to the web management portal. When parsing the WebFilterURLs 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-16140.	2023-03-29	6.8	Medium
CVE-2022-43624	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 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	Medium
CVE-2022-43625	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 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.	2023-03-29	6.8	Medium
CVE-2022-43626	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	2023-03-29	6.8	Medium

		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.			
CVE-2022-43627	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 SetStaticRouteIPv4Settings requests to the web management portal. When parsing subelements within the StaticRouteIPv4Data 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-16147.	2023-03-29	6.8	Medium
CVE-2022-43628	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 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 this vulnerability to execute code in the context of root. Was ZDI-CAN-16148.	2023-03-29	6.8	Medium
CVE-2022-43629	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 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 leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-16149.	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.	2023-03-29	6.8	Medium
CVE-2022-43632	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 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-2022-43633	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 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.	2023-03-29	6.8	Medium
CVE-2022-47529	rsa - netwitness	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 service configuration: to either disable it completely or run user-supplied code or commands, thereby bypassing tamper-protection features via ACL modification.	2023-03-28	6.7	Medium
CVE-2023-1073	linux - linux_kernel	A memory corruption flaw was found in the Linux kernel's human interface device (HID) subsystem in how a user inserts a malicious	2023-03-27	6.6	Medium

		USB device. This flaw allows a local user to crash or potentially escalate their privileges on the system.			
CVE-2023-25661	google - tensorflow	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 vulnerability.	2023-03-27	6.5	Medium
CVE-2022-48291	huawei - multiple products	The Bluetooth module has an authentication bypass vulnerability in the pairing process. Successful exploitation of this vulnerability may affect confidentiality.	2023-03-27	6.5	Medium
CVE-2022-48354	huawei - multiple products	The Bluetooth module has a heap out-of-bounds write vulnerability. Successful exploitation of this vulnerability can cause the Bluetooth process to crash.	2023-03-27	6.5	Medium
CVE-2022-48355	huawei - multiple products	The Bluetooth module has a heap out-of-bounds read vulnerability. Successful exploitation of this vulnerability can cause the Bluetooth process to crash.	2023-03-27	6.5	Medium
CVE-2022-24972	tp-link - tl-wr940n_firmware	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 stored credentials, leading to further compromise. Was ZDI-CAN-13911.	2023-03-28	6.5	Medium
CVE-2022-43635	tp-link - tl-wr940n_firmware	This vulnerability allows network-adjacent attackers to disclose 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 authentication algorithm. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-17332.	2023-03-29	6.5	Medium
CVE-2023-25197	apache - fineract	Improper Neutralization of Special Elements used in an SQL 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 apache fineract: from 1.4 through 1.8.2.	2023-03-28	6.3	Medium
CVE-2022-2237	redhat - multiple products	A flaw was found in the Keycloak Node.js Adapter. This flaw allows an attacker to benefit from an Open Redirect vulnerability in the checkSso function.	2023-03-27	6.1	Medium
CVE-2023-1074	linux - linux_kernel	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 denial of service.	2023-03-27	5.5	Medium
CVE-2023-1076	linux - linux_kernel	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 tun/tap sockets being incorrectly treated in filtering/routing decisions, possibly bypassing network filters.	2023-03-27	5.5	Medium
CVE-2023-25875	adobe - substance_3d_stager	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	Medium
CVE-2023-25876	adobe - substance_3d_stager	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	Medium
CVE-2023-25877	adobe - substance_3d_stager	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	Medium

		this issue requires user interaction in that a victim must open a malicious file.			
CVE-2023-25878	adobe - substance_3d_stager	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	Medium
CVE-2023-1637	linux - linux_kernel	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 attacks.	2023-03-27	5.5	Medium
CVE-2023-26338	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.	2023-03-28	5.5	Medium
CVE-2023-26339	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.	2023-03-28	5.5	Medium
CVE-2023-26340	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.	2023-03-28	5.5	Medium
CVE-2023-26341	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.	2023-03-28	5.5	Medium
CVE-2023-26342	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.	2023-03-28	5.5	Medium
CVE-2023-26343	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.	2023-03-28	5.5	Medium
CVE-2023-26344	adobe - dimension	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 this issue requires user interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
CVE-2023-26345	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.	2023-03-28	5.5	Medium
CVE-2023-26346	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.	2023-03-28	5.5	Medium
CVE-2023-26348	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.	2023-03-28	5.5	Medium
CVE-2023-26349	adobe - dimension	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 interaction in that a victim must open a malicious file.	2023-03-28	5.5	Medium
CVE-2023-26350	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.	2023-03-28	5.5	Medium
CVE-2023-26351	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	2023-03-28	5.5	Medium

		bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2023-26352	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.	2023-03-28	5.5	Medium
CVE-2023-26353	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.	2023-03-28	5.5	Medium
CVE-2023-26354	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.	2023-03-28	5.5	Medium
CVE-2023-26355	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.	2023-03-28	5.5	Medium
CVE-2023-26356	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.	2023-03-28	5.5	Medium
CVE-2023-1550	f5 - multiple products	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 Manager and used in conjunction with NGINX API Connectivity Manager, and NGINX Management Suite Security Monitoring.	2023-03-29	5.5	Medium
CVE-2023-28158	apache - archiva	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 some XSS content and gain some privileges such admin user.	2023-03-29	5.4	Medium
CVE-2022-1274	redhat - multiple products	A flaw was found in Keycloak in the execute-actions-email endpoint. This issue allows arbitrary HTML to be injected into emails sent to Keycloak users and can be misused to perform phishing or other attacks against users.	2023-03-29	5.4	Medium
CVE-2022-43473	zohocorp - multiple products	A blind XML External Entity (XXE) vulnerability exists in the Add UCS Device functionality of ManageEngine OpManager 12.6.168. A specially crafted XML file can lead to SSRF. An attacker can serve a malicious XML payload to trigger this vulnerability.	2023-03-30	5.4	Medium
CVE-2023-28866	linux - linux_kernel	In the Linux kernel through 6.2.8, net/bluetooth/hci_sync.c allows out-of-bounds access because amp_init1[] and amp_init2[] are supposed to have an intentionally invalid element, but do not.	2023-03-27	5.3	Medium
CVE-2023-22250	adobe - multiple products	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 minor feature. Exploitation of this issue does not require user interaction.	2023-03-27	5.3	Medium
CVE-2022-48361	huawei - multiple products	The Always On Display (AOD) has a path traversal vulnerability in theme files. Successful exploitation of this vulnerability may cause a failure in reading AOD theme resources.	2023-03-27	5.3	Medium
CVE-2023-0465	openssl - multiple products	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 `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.	2023-03-28	5.3	Medium
CVE-2023-0466	openssl - multiple products	The function X509_VERIFY_PARAM_add0_policy() is documented 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 deployments it was decided to keep the existing behavior of the 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.			
CVE-2023-22249	adobe - multiple products	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 inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2023-03-27	4.8	Medium
CVE-2022-42432	linux - linux_kernel	This vulnerability allows local attackers to disclose sensitive 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 kernel. Was ZDI-CAN-18540.	2023-03-29	4.4	Medium
CVE-2023-22251	adobe - multiple products	Adobe Commerce versions 2.4.4-p2 (and earlier) and 2.4.5-p1 (and earlier) are affected by an Incorrect Authorization vulnerability. A low-privileged authenticated attacker could leverage this vulnerability to achieve minor information disclosure.	2023-03-27	4.3	Medium
CVE-2023-25196	apache - fineract	Improper Neutralization of Special Elements used in an SQL 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 Apache Fineract: from 1.4 through 1.8.2.	2023-03-28	4.3	Medium
CVE-2022-27597	qnap - multiple products	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 vulnerabilities in the following operating system versions: QTS 5.0.1.2346 build 20230322 and later QuTS hero h5.0.1.2348 build 20230324 and later	2023-03-29	4.3	Medium
CVE-2022-27598	qnap - multiple products	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 vulnerabilities in the following operating system versions: QTS 5.0.1.2346 build 20230322 and later QuTS hero h5.0.1.2348 build 20230324 and later	2023-03-29	4.3	Medium
CVE-2022-1230	samsung - galaxy_s21_firmware	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 conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the current user. Was ZDI-CAN-15918.	2023-03-28	3.9	Low
CVE-2023-1075	linux - linux_kernel	A flaw was found in the Linux Kernel. The tls_is_tx_ready() incorrectly checks for list emptiness, potentially accessing a type confused entry to the list_head, leaking the last byte of the confused field that overlaps with rec->tx_ready.	2023-03-27	3.3	Low
CVE-2021-3923	linux - multiple products	A flaw was found in the Linux kernel's implementation of RDMA over infiniband. An attacker with a privileged local account can leak kernel stack information when issuing commands to the /dev/infiniband/rdma_cm device node. While this access is unlikely to leak sensitive user information, it can be further used to defeat existing kernel protection mechanisms.	2023-03-27	2.3	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.