

WHITE where information can be shared or published on any public forums.

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها Please note that this notification/advisory has been tagged as TLP أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للتُغرات المسجلة 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 11th الأسبوع من ١١ يونيو إلى National Vulnerability Database (NVD) of June to $17^{ ext{th}}$ of June. Vulnerabilities are scored using the Common معيار معيار معيار 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

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	CVSS Score	Severity
		Previous versions of HP Device Manager (prior to HPDM 5.0.10)			
	hp - multiple	could potentially allow command injection and/or elevation of			
CVE-2023-26295	products	privileges.	2023-06-12	9.8	Critical
		Certain versions of HP PC Hardware Diagnostics Windows, HP			
	hp - multiple	Image Assistant, and HP Thunderbolt Dock G2 Firmware are			
CVE-2023-32673	products	potentially vulnerable to elevation of privilege.	2023-06-12	9.8	Critical
	hp -				
ļ	pc_hardware_diagn	Certain versions of HP PC Hardware Diagnostics Windows are			
CVE-2023-32674	ostics	potentially vulnerable to buffer overflow.	2023-06-12	9.8	Critical
ļ		A plaintext storage of a password vulnerability [CWE-256] in			
ļ		FortiSIEM 6.7 all versions, 6.6 all versions, 6.5 all versions, 6.4 all			
	6	versions, 6.3 all versions, 6.2 all versions, 6.1 all versions, 5.4 all			
01/5 2022 20224	fortinet - multiple	versions, 5.3 all versions may allow an attacker able to access user	2022 06 42	0.0	0 1
CVE-2023-26204	products	DB content to impersonate any admin user on the device GUI.	2023-06-13	9.8	Critical
1		A heap-based buffer overflow vulnerability [CWE-122] in FortiOS			
1		version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3			
ļ		and below, version 7.0.9 and below, version 2.0.12 and below,			
ļ		version 1.2 all versions, version 1.1 all versions SSL-VPN may allow			
ļ	fortinet - multiple	a remote attacker to execute arbitrary code or commands via			
CVE-2023-27997	products	specifically crafted requests.	2023-06-13	9.8	Critical
<u> </u>	tp-link - tl-	TP-Link TL-WPA8630P (US)_ V2_ Version 171011 was discovered	2023 00 13	3.0	Circical
ļ	wpa8630p_firmwar	to contain a command injection vulnerability via the key			
CVE-2023-27837	e	parameter in the function sub_ 40A774.	2023-06-13	9.8	Critical
	tp-link - tl-	TP-Link TL-WPA8630P (US)_ V2_ Version 171011 was discovered			
	wpa8630p_firmwar	to contain a command injection vulnerability via the devicePwd			
CVE-2023-27836	e	parameter in the function sub_ 40A80C.	2023-06-13	9.8	Critical
	tp-link - tl-	TP-Link TL-WPA7510 (EU)_V2_190125 was discovered to contain a			
CVE-2023-29562	wpa7510_firmware	stack overflow via the operation parameter at /admin/locale.	2023-06-13	9.8	Critical
	microsoft -				
CVE-2023-29357	sharepoint_server	Microsoft SharePoint Server Elevation of Privilege Vulnerability	2023-06-14	9.8	Critical
	microsoft - multiple	Windows Pragmatic General Multicast (PGM) Remote Code			
CVE-2023-29363	products	Execution Vulnerability	2023-06-14	9.8	Critical
	microsoft - multiple	Windows Pragmatic General Multicast (PGM) Remote Code			
CVE-2023-32014	products	Execution Vulnerability	2023-06-14	9.8	Critical
1	microsoft - multiple	Windows Pragmatic General Multicast (PGM) Remote Code			
CVE-2023-32015	products	Execution Vulnerability	2023-06-14	9.8	Critical
CVE-2021-0701	google - android	Product: AndroidVersions: Android SoCAndroid ID: A-277775870	2023-06-15	9.8	Critical
CVE-2021-0945	google - android	Product: AndroidVersions: Android SoCAndroid ID: A-278156680	2023-06-15	9.8	Critical
1		In btm_ble_periodic_adv_sync_lost of btm_ble_gap.cc, there is a			
l l		possible remote code execution due to a buffer overflow. This			
1		could lead to remote code execution with no additional execution			
1		privileges needed. User interaction is not needed for			
CVE 2022 24422		exploitation.Product: AndroidVersions: Android-13Android ID: A-	2022 06 15	0.0	Correct to
CVE-2023-21130	google - android	273502002	2023-06-15	9.8	Critical
l l	tp-link -				
1		TD 1: - A AV40/EU)			
CVE-2023-34832	archer_ax10_firmw are	TP-Link Archer AX10(EU)_V1.2_230220 was discovered to contain a buffer overflow via the function FUN_131e8 - 0x132B4.	2023-06-16	9.8	Critical

CVE-2023-24470	microfocus - arcsight_logger	Potential XML External Entity Injection in ArcSight Logger versions prior to 7.3.0.	2023-06-13	9.1	Critical
CVL 2023 24470	dresignt_logger	The DBCPConnectionPool and HikariCPConnectionPool Controller	2023 00 13	3.1	Circical
		Services in Apache NiFi 0.0.2 through 1.21.0 allow an			
		authenticated and authorized user to configure a Database URL			
		with the H2 driver that enables custom code execution.			
		The resolution validates the Database URL and rejects H2 JDBC locations.			
		You are recommended to upgrade to version 1.22.0 or later which			
		fixes this issue.			
CVE-2023-34468	apache - nifi		2023-06-12	8.8	High
CVE-2023-28478	tp-link -	TP-Link EC-70 devices through 2.3.4 Build 20220902 rel.69498 have a Buffer Overflow.	2023-06-12	8.8	High
UVE-2023-28478	ec70_firmware	Previous versions of HP Device Manager (prior to HPDM 5.0.10)	2023-06-12	0.0	High
	hp - multiple	could potentially allow command injection and/or elevation of			
CVE-2023-26296	products	privileges.	2023-06-12	8.8	High
		Previous versions of HP Device Manager (prior to HPDM 5.0.10)			
CVE-2023-26297	hp - multiple products	could potentially allow command injection and/or elevation of privileges.	2023-06-12	8.8	Uiah
CVE-2023-20297	products	Previous versions of HP Device Manager (prior to HPDM 5.0.10)	2023-06-12	0.0	High
	hp - multiple	could potentially allow command injection and/or elevation of			
CVE-2023-26298	products	privileges.	2023-06-12	8.8	High
		An Improper Restriction of Excessive Authentication Attempts			
	fautions or details	[CWE-307] in FortiSIEM below 7.0.0 may allow a non-privileged			
CVE-2022-42478	fortinet - multiple products	user with access to several endpoints to brute force attack these endpoints.	2023-06-13	8.8	High
CVL-2022-42470	products	Insufficient verification of data authenticity in Zoom for Windows	2023-00-13	0.0	Iligii
		clients before 5.14.0 may allow an authenticated user to			
CVE-2023-34113	zoom - zoom	potentially enable an escalation of privilege via network access.	2023-06-13	8.8	High
		Improper input validation in the Zoom for Windows, Zoom			
	zaam multinla	Rooms, Zoom VDI Windows Meeting clients before 5.14.0 may			
CVE-2023-34121	zoom - multiple products	allow an authenticated user to potentially enable an escalation of privilege via network access.	2023-06-13	8.8	High
042 2020 0 1121	products	Use after free in Autofill payments in Google Chrome prior to	2020 00 10	0.0	
		114.0.5735.133 allowed a remote attacker to potentially exploit			
		heap corruption via a crafted HTML page. (Chromium security			
CVE-2023-3214	google - chrome	severity: Critical)	2023-06-13	8.8	High
		Use after free in WebRTC in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit			
		heap corruption via a crafted HTML page. (Chromium security			
CVE-2023-3215	google - chrome	severity: High)	2023-06-13	8.8	High
		Type confusion in V8 in Google Chrome prior to 114.0.5735.133			
CVE-2023-3216	google - chrome	allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-13	8.8	Uiah
<u>CVE-2023-3210</u>	google - cilionie	Use after free in WebXR in Google Chrome prior to 114.0.5735.133	2023-00-13	0.0	High
		allowed a remote attacker to potentially exploit heap corruption			
CVE-2023-3217	google - chrome	via a crafted HTML page. (Chromium security severity: High)	2023-06-13	8.8	High
	microsoft - multiple				
CVE-2023-29362	products	Remote Desktop Client Remote Code Execution Vulnerability	2023-06-14	8.8	High
CVE-2023-29372	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2023-06-14	8.8	High
CVL 2023 23372	microsoft - multiple	Execution value ability	2023 00 14	0.0	riigii
CVE-2023-29373	products	Microsoft ODBC Driver Remote Code Execution Vulnerability	2023-06-14	8.8	High
	microsoft - multiple	Windows Collaborative Translation Framework Elevation of			
CVE-2023-32009	products	Privilege Vulnerability	2023-06-14	8.8	High
CVE-2023-33131	microsoft - multiple products	Microsoft Outlook Remote Code Execution Vulnerability	2023-06-14	8.8	High
<u> </u>	microsoft - multiple	The Sour Outlook Remote Code Execution Vullerability	2020 00 14	0.0	111511
CVE-2023-32031	products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-06-14	8.8	High
		IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 could allow			
	ibm -	a remote authenticated attacker to execute arbitrary commands			
CVE-2022-32752	security_directory_	on the system by sending a specially crafted request. IBM X-Force	2023-06-15	8.8	مام:ایا
CVE-2UZZ-3Z/3Z	suite_va	ID: 228439. Cross-site request forgery (CSRF) vulnerability in the Layout	2023-00-15	0.0	High
		module's SEO configuration in Liferay Portal 7.4.3.70 through			
		7.4.3.76, and Liferay DXP 7.4 update 70 through 76 allows remote			
		attackers to execute arbitrary code in the scripting console via the			
CVE 2022 25020	liferay - multiple	`_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_ba	2022 00 45	0.0	11:-1
CVE-2023-35030	products	ckURL` parameter. In sdpu_build_uuid_seq of sdp_discovery.cc, there is a possible	2023-06-15	8.8	High
		out of bounds write due to a use after free. This could lead to			
		remote code execution over Bluetooth, if HFP support is enabled,			
		with no additional execution privileges needed. User interaction is			
	مامناهانيمن ماميميما	not needed for exploitation.Product: AndroidVersions: Android-11			1
OVE 2022 24122	google - multiple	·	2022 20 1-	0.0	
CVE-2023-21108	products google - multiple google - multiple	Android-12 Android-12L Android-13Android ID: A-239414876 In btm_sec_encrypt_change of btm_sec.cc, there is a possible way	2023-06-15	8.8	High

		This could lead to paired device escalation of privilege with no			
		additional execution privileges needed. User interaction is not			
		needed for exploitation.Product: AndroidVersions: Android-11			
		Android-12 Android-12LAndroid ID: A-258834033			
		In readSampleData of NuMediaExtractor.cpp, there is a possible out of bounds write due to uninitialized data. This could lead to			
		remote code execution with no additional execution privileges			
		needed. User interaction is needed for exploitation. Product:			
	google - multiple	AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-21127	products	13Android ID: A-275418191	2023-06-15	8.8	High
		<pre><div data-wrapper="true" style="font-family:'Segoe UI','Helvetica Neue',sans-serif; font-size:9pt"></div></pre>			
		<pre><div>Windows Server Service Security Feature Bypass</div></pre>			
	microsoft - multiple	Vulnerability			
CVE-2023-32022	products		2023-06-14	8.6	High
		SAP UI5 Variant Management - versions SAP_UI 750, SAP_UI 754,			
		SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, does not			
		sufficiently encode user-controlled inputs on reading data from the server, resulting in Stored Cross-Site Scripting (Stored XSS)			
		vulnerability. After successful exploitation, an attacker with user			
		level access can cause high impact on confidentiality, modify some			
	sap - multiple	information and can cause unavailability of the application at user			
CVE-2023-33991	products	level.	2023-06-13	8.2	High
		Uncontrolled search path element vulnerability in Backup Management Functionality in Synology DiskStation Manager			
	synology - multiple	(DSM) before 7.1-42661 allows remote authenticated users to			
CVE-2023-0142	products	read or write arbitrary files via unspecified vectors.	2023-06-13	8.1	High
	microsoft - multiple				
CVE-2023-29351	products	Windows Group Policy Elevation of Privilege Vulnerability	2023-06-14	8.1	High
CVE-2023-35142	jenkins - checkmarx	Jenkins Checkmarx Plugin 2022.4.3 and earlier disables SSL/TLS validation for connections to the Checkmarx server by default.	2023-06-14	8.1	⊔iαh
CVE-2023-33142	ibm -	IBM Security Directory Suite VA 8.0.1 specifies permissions for a	2023-00-14	0.1	High
	security directory	security-critical resource in a way that allows that resource to be			
CVE-2022-33163	suite_va	read or modified by unintended actors. IBM X-Force ID: 228571.	2023-06-15	8.1	High
		In Jenkins 2.399 and earlier, LTS 2.387.3 and earlier, POST requests			
		are sent in order to load the list of context actions. If part of the			
	jenkins - multiple	URL includes insufficiently escaped user-provided values, a victim may be tricked into sending a POST request to an unexpected			
CVE-2023-35141	products	endpoint by opening a context menu.	2023-06-14	8	High
011 1010 00111	microsoft - multiple	enapoint by opening a context mena.	2023 00 11	0	6
CVE-2023-28310	products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-06-14	8	High
		Previous versions of HP Device Manager (prior to HPDM 5.0.10)			
CVE 2022 26204	hp - multiple	could potentially allow command injection and/or elevation of	2022 06 42	7.0	11:-1-
CVE-2023-26294	products	Privileges. A use of externally-controlled format string in Fortinet FortiOS	2023-06-12	7.8	High
		version 7.2.0 through 7.2.4, FortiOS all versions 7.0, FortiOS all			
		versions 6.4, FortiOS all versions 6.2, FortiProxy version 7.2.0			
		through 7.2.1, FortiProxy version 7.0.0 through 7.0.7 allows			
	fortinet - multiple	attacker to execute unauthorized code or commands via specially			
CVE-2022-43953	products	crafted commands.	2023-06-13	7.8	High
		A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0			
		through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0,			
		FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0			
		through 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions			
		1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows			
CVE 2022 22C20	fortinet - multiple	attacker to escalation of privilege via specifically crafted	2022 06 42	7.0	11:
CVE-2023-22639	products	commands. Multiple improper neutralization of special elements used in an os	2023-06-13	7.8	High
		command ('OS Command Injection') vulnerabilties [CWE-78] in			
		Fortinet FortiADCManager version 7.1.0 and before 7.0.0,			
		FortiADC version 7.2.0 and before 7.1.2 allows a local			
	fortinet - multiple	authenticated attacker to execute arbitrary shell code as `root`			
CVE-2023-26210	products	user via crafted CLI requests.	2023-06-13	7.8	High
		An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC CLI 7.1.0, 7.0.0			
		through 7.0.3, 6.2.0 through 6.2.4, 6.1 all versions, 6.0 all versions			
		may allow a local and authenticated attacker to execute			
	fortinet - multiple	unauthorized commands via specifically crafted arguments in			
CVE-2023-28000	products	diagnose system df CLI command.	2023-06-13	7.8	High
		Improper privilege management in Zoom for Windows, Zoom			
		Rooms for Windows, and Zoom VDI for Windows clients before			
	700m	5.14.0 may allow an authenticated user to potentially enable an			
	zoom - virtual_desktop_inf	escalation of privilege via local access. Users may potentially utilize higher level system privileges maintained by the Zoom client to			
	. VIILUUI UESKLUU III				Hiah
CVE-2023-34120		spawn processes with escalated privileges.	2023-06-13	7.8	∐l⊼u
CVE-2023-34120	rastructure	spawn processes with escalated privileges. Improper input validation in the installer for Zoom for Windows	2023-06-13	7.8	High
CVE-2023-34120			2023-06-13	7.8	півіі

Microsoft - multiple products Microsoft - multiple product	CVE-2023-29346	microsoft - multiple products	NTFS Elevation of Privilege Vulnerability	2023-06-14	7.8	High
CVS-2023-20390 microsoft - multiple products of providers with products of pro	CVE 2022 20259	· ·		2022 06 14	7.0	
Windows PM Device Driver Elevation of Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Media Bernote Code Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Media Bernote Code Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Media Bernote Code Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Media Bernote Code Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Media Bernote Code Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation of Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation of Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation of Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation of Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Privilege Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows Soft Elevation Vulnerability 2023-06-14 7,8 High microsoft multiple products Windows	CVE-2023-29358	'	windows GDI Elevation of Privilege vulnerability	2023-06-14	7.8	High
Viv. 2023-20256 products windows FIPM Device Driver Elevation of Printinge Vulnerability 2023-06-14 7,8 High microsoft multiple products windows Media Amonte Code Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products windows Geolociation Service Remote Code Execution 2023-06-14 7,8 High microsoft multiple products windows Geolociation Service Remote Code Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products windows Good Execution Vulnerability 2023-06-14 7,8 High microsoft multiple products windows Good Elevation of Privilege Vulnerability windows Good Elevation Vulnerability windows Helia Remote Code Execution Vulnerability windows Heli	CVE-2023-29359	•	GDI Elevation of Privilege Vulnerability	2023-06-14	7.8	High
Viv. 2023-2036 products Windows Media Remote Code Execution Vulnerability 2023-06-14 7.8 High microsoft-multiple products Vulnerability Vuln	CVE-2023-29360	products	Windows TPM Device Driver Elevation of Privilege Vulnerability	2023-06-14	7.8	High
Microsoft - multiple products Windows Seelocation Service Remote Code Execution 2023 06-14 7.8 High	CVE-2022-20265		Windows Media Remote Code Execution Vulnerability	2022-06-14	7 0	Hiαh
CVE-2023-2936 Microsoft - multiple products -	CVE-2023-29303	· · · · · · · · · · · · · · · · · · ·	,	2025-00-14	7.0	півіі
CVE-2023-29379 products microsoft - multiple multiple multiple - multiple multiple multiple - mult	CVE-2023-29366	•	Vulnerability	2023-06-14	7.8	High
CV-2023-29370 products microsoft -multiple CV-2023-29370 products microsoft -multiple CV-2023-29370 products microsoft -multiple CV-2023-29300 products microsoft -multiple CV-2023-29012 products microsoft -multiple CV-2023-29012 products microsoft -multiple CV-2023-29012 products microsoft -multiple CV-2023-29012 products microsoft -multiple products multiple pr	CVE-2023-29367	products	iSCSI Target WMI Provider Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-29371 microsoft - multiple products	CVE-2023-29370	'	Windows Media Remote Code Execution Vulnerability	2023-06-14	7.8	High
windows Resilient File System (Refs) Remote Code Execution Valenzability Valenz	CVE 2022 20274	microsoft - multiple	·	2022 06 14		
CVE-2023-32018 products microsoft multiple vice-2023-32017 microsoft multiple vice-2023-32017 microsoft multiple vice-2023-32018 microsoft multiple vice-2023-32018 microsoft multiple vice-2023-32018 microsoft multiple vice-2023-32018 microsoft multiple vice-2023-32019 microsoft multiple vice-2023-2023 micro	CVE-2023-29371	· · · · · · · · · · · · · · · · · · ·		2023-06-14	7.8	High
CVE-2023-32012 products microsoft multiple microsof	CVE-2023-32008	products	Vulnerability	2023-06-14	7.8	High
CVE_2023_32012 microsoft - multiple products volunerability volune	CVE-2023-32012	· ·		2023-06-14	7.8	High
Windows Hello Remote Code Execution Vulnerability 2023-06-14 7.8 High		microsoft - multiple	Microsoft PostScript Printer Driver Remote Code Execution			
Windows Hello Remote Code Execution Vulnerability 2023-06-14 7.8 High	CVE-2023-32017	· · · · · · · · · · · · · · · · · · ·	Vulnerability	2023-06-14	7.8	High
Microsoft = Multiple products Microsoft Excel Remote Code Execution Vulnerability 2023-06-14 7.8 High Microsoft = Microsoft Excel Remote Code Execution Vulnerability 2023-06-14 7.8 High Microsoft = Microsoft	CVE-2023-32018	products	Windows Hello Remote Code Execution Vulnerability	2023-06-14	7.8	High
Microsoft - multiple products Microsoft Excel Remote Code Execution Vulnerability 2023-06-14 7.8 High Microsoft Description Microsoft Descriptio	CVE-2023-32029	· ·	Microsoft Excel Remote Code Execution Vulnerability	2023-06-14	7.8	High
Microsoft - multiple products microsoft - multiple products microsoft - multiple products microsoft - multiple microsoft		microsoft - multiple				
Products Microsoft Excel Remote Code Execution Vulnerability 2023-06-14 7.8 High microsoft - multiple products Microsoft Office Remote Code Execution Vulnerability 2023-06-14 7.8 High A CWE-94: Improper Control of Generation of Code ("Code Injection") vulnerability exists that could cause execution of malicious code when an unsuspicious schneider-electric multiple products of multiple products of a CWE-787: Out-of-Bounds Write vulnerability exists that could cause execution of malicious code when an unsuspicious schneider-electric ecostruxure foxbor og. dcs. control core services og. dcs. control core services og. dcs. control core costruxure, foxbor og. dcs. control core services og. dcs. control core costruxure, foxbor og. dcs. control core services og. dcs. control core services og. dcs. control core costruxure, foxbor og. dcs. control core services og. dcs. control core costruxure, foxbor og. dcs. control core services og. dcs. control core costruxure, foxbor og. dcs. control core services og. dcs. control core costruxure, foxbor og. dcs. control core services og. dcs. control core costruxure foxbor og. dcs. control core services og. dcs. control core costruxure foxbor og. dcs. control core costruxure foxbor og. dcs. control core services og. dcs. control core costruxure foxbor og. dcs. dcs. dcs. dcs. dcs. dcs. dcs. dcs	CVE-2023-33133	·	Microsoft Excel Remote Code Execution Vulnerability	2023-06-14	7.8	High
A CWE-1923-33146 products Microsoft Office Remote Code Execution Vulnerability 2023-06-14 7.8 High	CVE-2023-33137	products	Microsoft Excel Remote Code Execution Vulnerability	2023-06-14	7.8	High
Injection') vulnerability exists that could cause execution of malicious code when an unsuspicious user loads a project file from the local filesystem into the HMI. 2023-06-14 7.8 High	CVE-2023-33146	· ·	Microsoft Office Remote Code Execution Vulnerability	2023-06-14	7.8	High
O_dcs_control_core services	CVE-2023-1049	multiple products schneider-electric -	could cause execution of malicious code when an unsuspicious user loads a project file from the local filesystem into the HMI. A CWE-787: Out-of-Bounds Write vulnerability exists that could cause local denial-of-service, elevation of privilege, and potentially kernel execution when a	2023-06-14	7.8	High
A CWE-129: Improper Validation of Array Index vulnerability exists that could cause local denial-of-service, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an unpredictable index to an IOCTL call in the Foxboro.sys driver. CVE-2023-2570 A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. CVE-2023-24895 CVE-2023-24895 CVE-2023-24897 Incrosoft - Inet_framework without an interpretation of Missual Studio Remote Code Execution Vulnerability without an interpretation of Missual Studio Remote Code Execution Vulnerability without microsoft - Inet_framework without without microsoft - Inet_framework without witho		_				
that could cause local denial-of-service, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an unpredictable index to an IOCTL call in the Foxboro.sys driver. CVE-2023-2570 A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. CVE-2023-24895 Inet_framework Microsoft - Inet_framework Vulnerability Microsoft - Inet_framework Vulnerability Microsoft - Inet_framework NET, NET Framework, and Visual Studio Remote Code Execution Vulnerability Microsoft - Inet_framework NET, NET Framework, and Visual Studio Remote Code Execution Vulnerability Microsoft - Inet_framework NET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MICrosoft - Inet_framework MET Framework Remote Code Execution Vulnerability Microsoft - Inet_framework MICrosoft - Inet_framework MICrosoft - Inet_framework MICrosoft - I	CVE-2023-2569			2023-06-14	7.8	High
in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. CVE-2023-2001	CVE-2023-2570	ecostruxure_foxbor o_dcs_control_core	that could cause local denial-of-service, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an unpredictable index to an IOCTL	2023-06-14	7.8	High
in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file. CVE-2023-2001			A CWF-502: Desertalization of Untrusted Data vulnerability exists			
microsoftnet_framework			in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code			
CVE-2023-24895 .net_framework microsoftnet_framework vulnerability .net_framework vulnerability .net_framework vulnerability .net_framework vulnerability .net_framework vulnerability .net_framework	CVE-2023-3001			2023-06-14	7.8	High
CVE-2023-24897 .net_framework	CVE-2023-24895	.net_framework	Vulnerability	2023-06-14	7.8	High
.net_framework	CVE-2023-24897			2023-06-14	7.8	High
IBM Security Guardium 11.3, 11.4, and 11.5 could allow a local user to obtain elevated privileges due to incorrect authorization checks. IBM X-Force ID: 216753. In multiple functions of cdm_engine.cpp, there is a possible useafter-free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	CVE. 2022 2022C		NET Framework Pamete Code Evecution Vulnerability	2022 06 14	7.0	Lliah
CVE-2022-22307 products checks. IBM X-Force ID: 216753. 2023-06-15 7.8 High In multiple functions of cdm_engine.cpp, there is a possible use- after-free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	<u>CVE-2U23-2932b</u>	.net_iramework	,	2023-06-14	7.8	nign
In multiple functions of cdm_engine.cpp, there is a possible use- after-free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	CVE 2022 22207	· ·	user to obtain elevated privileges due to incorrect authorization	2022 06 45	7.0	11! =1-
needed. User interaction is not needed for exploitation.Product:	<u>CVE-ZUZZ-ZZ3U/</u>	products	In multiple functions of cdm_engine.cpp, there is a possible use-after-free due to improper locking. This could lead to local	2023-06-15	7.8	нıgn
	01/5 2000 2000		needed. User interaction is not needed for exploitation.Product:	2022 22 :=		

		I. 5			
		In onResume of AppManagementFragment.java, there is a possible way to prevent users from forgetting a previously			
		connected VPN due to improper input validation. This could lead			
		to local escalation of privilege with no additional execution			
		privileges needed. User interaction is not needed for			
	google - multiple	exploitation.Product: AndroidVersions: Android-11 Android-			
CVE-2023-21121	products	12Android ID: A-205460459	2023-06-15	7.8	High
		In various functions of various files, there is a possible way to			
		bypass the DISALLOW_DEBUGGING_FEATURES restriction for			
		tracing due to a missing permission check. This could lead to local			
		escalation of privilege with no additional execution privileges			
	googlo multiplo	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-21122	google - multiple products	13Android ID: A-270050191	2023-06-15	7.8	High
CVE-2023-21122	products	In multiple functions of multiple files, there is a possible way to	2023-00-13	7.0	півп
		bypass the DISALLOW_DEBUGGING_FEATURES restriction for			
		tracing due to a missing permission check. This could lead to local			
		escalation of privilege with no additional execution privileges			
		needed. User interaction is not needed for exploitation.Product:			
	google - multiple	AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-21123	products	13Android ID: A-270050064	2023-06-15	7.8	High
		In run of multiple files, there is a possible escalation of privilege			
		due to unsafe deserialization. This could lead to local escalation of			
		privilege with no additional execution privileges needed. User			
		interaction is not needed for exploitation.Product:			
	google - multiple	AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-21124	products	13Android ID: A-265798353	2023-06-15	7.8	High
		In bindOutputSwitcherAndBroadcastButton of			
		MediaControlPanel.java, there is a possible launch arbitrary			
		activity under SysUI due to Unsafe Intent. This could lead to local			
		escalation of privilege with no additional execution privileges			
C) /F 2022 24426		needed. User interaction is not needed for exploitation.Product:	2022 06 45	7.0	112.1
CVE-2023-21126	google - android	AndroidVersions: Android-13Android ID: A-271846393	2023-06-15	7.8	High
		In various functions of AppStandbyController.java, there is a			
		possible way to break manageability scenarios due to a logic error in the code. This could lead to local escalation of privilege with no			
		additional execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation.Product: AndroidVersions: Android-11			
CVE-2023-21128	products	Android-12 Android-12L Android-13Android ID: A-272042183	2023-06-15	7.8	High
<u>CVL 2023 21120</u>	products	In getFullScreenIntentDecision of	2023 00 13	7.0	111811
		NotificationInterruptStateProviderImpl.java, there is a possible			
		activity launch while the app is in the background due to a BAL			
		bypass. This could lead to local escalation of privilege with no			
		additional execution privileges needed. User interaction is needed			
	google - multiple	for exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2023-21129	products	Android-12L Android-13Android ID: A-274759612	2023-06-15	7.8	High
		In checkKeyIntentParceledCorrectly() of			
		ActivityManagerService.java, there is a possible bypass of Parcel			
		Mismatch mitigations due to a logic error in the code. This could			
		lead to local escalation of privilege and the ability to launch			
		arbitrary activities in settings with no additional execution			
		privileges needed. User interaction is not needed for			
CVE 2022 24424	google - multiple	exploitation.Product: AndroidVersions: Android-11 Android-12	2022 26 45	7.0	131.1
CVE-2023-21131	products	Android-12L Android-13Android ID: A-265015796	2023-06-15	7.8	High
		In onCreate of NotificationAccessSettings.java, there is a possible			
		failure to persist notifications settings due to improper input			
		validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation.Product: AndroidVersions: Android-11			
CVE-2023-21135	googie - multiple products	Android-12 Android-12L Android-13Android ID: A-260570119	2023-06-15	7.8	High
<u>CAF 5052-51122</u>	products	In onNullBinding of CallRedirectionProcessor.java, there is a	2023 00-13	7.0	ııığıı
		possible long lived connection due to improper input validation.			
		This could lead to local escalation of privilege and background			
		activity launches with User execution privileges needed. User			
		interaction is not needed for exploitation.Product:			
	google - multiple	AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-21138	products	13Android ID: A-273260090	2023-06-15	7.8	High
		In bindPlayer of MediaControlPanel.java, there is a possible launch			
		arbitrary activity in SysUI due to Unsafe Intent. This could lead to			
		local escalation of privilege with no additional execution privileges			
		needed. User interaction is not needed for exploitation.Product:			
01/5 0000 01/00	google - android	AndroidVersions: Android-13Android ID: A-271845008	2023-06-15	7.8	High
CVE-2023-21139		Microsoft ODBC Driver for SQL Server Remote Code Execution			
	microsoft - multiple	Land Later			High
CVE-2023-21139 CVE-2023-32027	products	Vulnerability	2023-06-16	7.8	riigii
CVE-2023-32027	products microsoft - multiple				
	products	Microsoft OLE DB Remote Code Execution Vulnerability	2023-06-16	7.8	High
CVE-2023-32027	products microsoft - multiple	Microsoft OLE DB Remote Code Execution Vulnerability An issue was discovered in fl_set_geneve_opt in			
CVE-2023-32027	products microsoft - multiple	Microsoft OLE DB Remote Code Execution Vulnerability			

		TCA_FLOWER_KEY_ENC_OPTS_GENEVE packets. This may result in			
		denial of service or privilege escalation.			
		Zoom for Windows clients prior to 5.13.5 contain an improper verification of cryptographic signature vulnerability. A malicious			
		user may potentially downgrade Zoom Client components to			
CVE-2023-28602	zoom - zoom	previous versions.	2023-06-13	7.7	High
		Use of insufficiently random values vulnerability in User			
		Management Functionality in Synology DiskStation Manager			
	synology - multiple	(DSM) before 7.2-64561 allows remote attackers to obtain user			
CVE-2023-2729	products	credential via unspecified vectors.	2023-06-13	7.5	High
		A use of a broken or risky cryptographic algorithm [CWE-327] in			
		Fortinet FortiSIEM before 6.7.1 allows a remote unauthenticated			
	fortinet - multiple	attacker to perform brute force attacks on GUI endpoints via			
CVE-2022-43949	products	taking advantage of outdated hashing methods.	2023-06-13	7.5	High
		An improper permissions, privileges, and access controls			
		vulnerability [CWE-264] in FortiNAC-F 7.2.0, FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.0 all versions 8.7.0 all			
	fortinet - multiple	versions may allow an unauthenticated attacker to perform a DoS			
CVE-2023-22633	products	attack on the device via client-secure renegotiation.	2023-06-13	7.5	High
<u> </u>	microsoft - multiple	attack on the device via them seedile renegotiation.	2023 00 13	7.5	8
CVE-2023-32011	products	Windows iSCSI Discovery Service Denial of Service Vulnerability	2023-06-14	7.5	High
<u> </u>	products	Exposure of Sensitive Information to an Unauthorized Actor	2023 00 11	7.0	6
	apache - multiple	vulnerability in Apache Software Foundation Apache Traffic			
CVE-2022-47184	products	Server.This issue affects Apache Traffic Server: 8.0.0 to 9.2.0.	2023-06-14	7.5	High
		Improper Input Validation vulnerability in Apache Software			
		Foundation Apache Traffic Server. The configuration			
		option proxy.config.http.push_method_enabled didn't			
		function. However, by default the PUSH method is blocked in the			
		ip_allow configuration file. This issue affects Apache Traffic Server:			
		from 8.0.0 through 9.2.0.			
DVE 2022 20624	apache - multiple	8.x users should upgrade to 8.1.7 or later versions	2022 25 4 4		
CVE-2023-30631	products	9.x users should upgrade to 9.2.1 or later versions	2023-06-14	7.5	High
		Exposure of Sensitive Information to an Unauthorized Actor			
		vulnerability in Apache Software Foundation Apache Traffic Server. This issue affects Apache Traffic Server: from 8.0.0 through			
		9.2.0.			
		3.2.0.			
	apache - multiple	8.x users should upgrade to 8.1.7 or later versions			
CVE-2023-33933	products	9.x users should upgrade to 9.2.1 or later versions	2023-06-14	7.5	High
	p. 66.6.65	Allocation of Resources Without Limits or Throttling vulnerability		7.10	6
		in Apache Software Foundation Apache Struts. This issue affects			
		Apache Struts: through 2.5.30, through 6.1.2.			
	apache - multiple				
CVE-2023-34396	products	Upgrade to Struts 2.5.31 or 6.1.2.1 or greater	2023-06-14	7.5	High
	microsoft -	.NET, .NET Framework, and Visual Studio Elevation of Privilege			
CVE-2023-24936	.net_framework	Vulnerability	2023-06-14	7.5	High
	microsoft -	.NET, .NET Framework, and Visual Studio Denial of Service			
CVE-2023-29331	.net_framework	Vulnerability	2023-06-14	7.5	High
	microsoft -				
CVE-2023-32030	.net_framework	.NET and Visual Studio Denial of Service Vulnerability	2023-06-14	7.5	High
		IBM PowerVM Hypervisor FW950.00 through FW950.71,			
		FW1010.00 through FW1010.40, FW1020.00 through FW1020.20,			
		and FW1030.00 through FW1030.11 could allow an attacker to			
N. F. 0055 5=5	ibm - multiple	obtain sensitive information if they gain service access to the HMC.	2005 5		
CVE-2023-25683	products	IBM X-Force ID: 247592.	2023-06-15	7.5	High
	ibm -	IBM Security Directory Suite VA 8.0.1 could allow an attacker to			
N/F 2022 22460	security_directory_	cause a denial of service due to uncontrolled resource	2022 25 45		
CVE-2022-33168	suite_va	consumption. IBM X-Force ID: 228588.	2023-06-15	7.5	High
	ile	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 uses an			
	ibm - security directory	inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID:			
CVE-2022-32757	suite_va	228510.	2023-06-15	7.5	High
2022 32131	Juice_va	In doInBackground of NotificationContentInflater.java, there is a	2020 00 10	,.5	11151
		possible temporary denial or service due to long running			
		operations. This could lead to remote denial of service with no			
		additional execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation.Product: AndroidVersions: Android-11			
CVE-2023-21144	products	Android-12 Android-12L Android-13Android ID: A-252766417	2023-06-15	7.5	High
	p. 234363	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and			·
		earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect			
		Authorization vulnerability that could result in a security feature			
		bypass. An attacker could leverage this vulnerability to leak			
	adobe - multiple	another user's data. Exploitation of this issue does not require user			
	products	interaction.	2023-06-15	7.5	High
CVE-2023-22248					
CVE-2023-22248	microsoft - multiple			l	
CVE-2023-22248 CVE-2023-33126	·	.NET and Visual Studio Remote Code Execution Vulnerability	2023-06-14	7.3	High
	microsoft - multiple	.NET and Visual Studio Remote Code Execution Vulnerability	2023-06-14	7.3	High

					1
CVE-2023-33130	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	2023-06-14	7.3	High
<u> </u>	microsoft - multiple	The state of the server speeding value about y		,.5	
CVE-2023-33135	products	.NET and Visual Studio Elevation of Privilege Vulnerability	2023-06-14	7.3	High
		An access control vulnerability [CWE-284] in FortiNAC version 9.4.2 and below, version 9.2.7 and below, 9.1 all versions, 8.8 all			
		versions, 8.7 all versions, 8.6 all versions, 8.5 all versions may allow			
	fortinet - multiple	a remote attacker authenticated on the administrative interface to			
CVE-2022-39946	products	perform unauthorized jsp calls via crafted HTTP requests.	2023-06-13	7.2	High
	ibm -	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 could allow a privileged user to upload malicious files of dangerous types that			
	security_directory_	can be automatically processed within the product's environment.			
CVE-2022-33166	suite_va	IBM X-Force ID: 228586.	2023-06-15	7.2	High
		Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Improper			
		Neutralization of Special Elements Used in a Template Engine			
		vulnerability that could lead to arbitrary code execution by an			
CVE 2022 20207	adobe - multiple	admin-privilege authenticated attacker. Exploitation of this issue	2022 06 45	7.0	11:
CVE-2023-29297	products zoom -	does not require user interaction. Zoom VDI client installer prior to 5.14.0 contains an improper	2023-06-15	7.2	High
	virtual_desktop_inf	access control vulnerability. A malicious user may potentially			
CVE-2023-28603	rastructure	delete local files without proper permissions.	2023-06-13	7.1	High
CVE 2022 245C5	microsoft - multiple	Azura DayOng Sanyar Speeding Wulpershilltu	2022 06 44	71	⊔i∼h
CVE-2023-21565	products microsoft - multiple	Azure DevOps Server Spoofing Vulnerability Windows SMB Witness Service Security Feature Bypass	2023-06-14	7.1	High
CVE-2023-32021	products	Vulnerability	2023-06-14	7.1	High
0.45 0000 0000	microsoft - multiple		2022 22 2		
CVE-2023-29337	products microsoft - multiple	NuGet Client Remote Code Execution Vulnerability Windows Cloud Files Mini Filter Driver Elevation of Privilege	2023-06-14	7.1	High
CVE-2023-29361	products	Vulnerability	2023-06-14	7	High
	microsoft - multiple				
CVE-2023-29364	products microsoft - multiple	Windows Authentication Elevation of Privilege Vulnerability	2023-06-14	7	High
CVE-2023-29368	products	Windows Filtering Platform Elevation of Privilege Vulnerability	2023-06-14	7	High
	microsoft - multiple	,			
CVE-2023-32010	products	Windows Bus Filter Driver Elevation of Privilege Vulnerability	2023-06-14	7	High
		In multiple functions of WVDrmPlugin.cpp, there is a possible use after free due to a race condition. This could lead to local			
		escalation of privilege with no additional execution privileges			
		needed. User interaction is not needed for exploitation.Product:		_	
CVE-2023-21101	google - android	AndroidVersions: Android SoCAndroid ID: A-258189255 A use after free issue was discovered in driver/firewire in	2023-06-15	7	High
		outbound_phy_packet_callback in the Linux Kernel. In this flaw a			
01/5 2022 2450	linux - multiple	local attacker with special privilege may cause a use after free	2022 05 42	6.7	
CVE-2023-3159	products microsoft -	problem when queue_event() fails.	2023-06-12	6.7	Medium
CVE-2023-33144	visual_studio_code	Visual Studio Code Spoofing Vulnerability	2023-06-14	6.6	Medium
		The JndiJmsConnectionFactoryProvider Controller Service, along		_	
		with the ConsumeJMS and PublishJMS Processors, in Apache NiFi 1.8.0 through 1.21.0 allow an authenticated and authorized user			
		to configure URL and library properties that enable deserialization			
		of untrusted data from a remote location.			
		The resolution validates the JNDI URL and restricts locations to a			
		set of allowed schemes.			
		Vou are recommended to warmed to the size of 22.0 districts			
CVE-2023-34212	apache - nifi	You are recommended to upgrade to version 1.22.0 or later which fixes this issue.	2023-06-12	6.5	Medium
	,	A server-side request forgery (SSRF) vulnerability [CWE-918]			
		in FortiManager and FortiAnalyzer GUI 7.2.0 through 7.2.1, 7.0.0			
	fortinet - multiple	through 7.0.6, 6.4.8 through 6.4.11 may allow a remote and authenticated attacker to access unauthorized files and services on			
CVE-2023-25609	products	the system via specially crafted web requests.	2023-06-13	6.5	Medium
		An insertion of sensitive information into log file vulnerability in			
	fortinet - multiple	Fortinet FortiOS 7.2.0 through 7.2.4 and FortiProxy 7.0.0 through 7.0.10. 7.2.0 through 7.2.1 allows an attacker to read certain			
CVE-2023-26207	products	passwords in plain text.	2023-06-13	6.5	Medium
		A loop with unreachable exit condition ('infinite loop') in Fortinet			
		FortiOS version 7.2.0 through 7.2.4, FortiOS version 7.0.0 through 7.0.10, FortiOS 6.4 all versions, FortiOS 6.2 all versions, FortiOS 6.0			
		all versions, FortiProxy version 7.2.0 through 7.2.3, FortiProxy			
		version 7.0.0 through 7.0.9, FortiProxy 2.0 all versions, FortiProxy			
		1.2 all versions, FortiProxy 1.1 all versions, FortiProxy 1.0 all			
		versions, FortiWeb version 7.2.0 through 7.2.1, FortiWeb version 7.0.0 through 7.0.6, FortiWeb 6.4 all versions, FortiWeb 6.3 all			
	fortinet - multiple	versions allows attacker to perform a denial of service via specially			
CVE-2023-33305	products	crafted HTTP requests.	2023-06-13	6.5	Medium

CVE-2023-28598	zoom - zoom	Zoom for Linux clients prior to 5.13.10 contain an HTML injection vulnerability. If a victim starts a chat with a malicious user it could result in a Zoom application crash.	2023-06-13	6.5	Medium
		Zoom for Windows clients prior to 5.14.0 contain an improper restriction of operations within the bounds of a memory buffer vulnerability. A malicious user may alter protected Zoom Client memory buffer potentially causing integrity issues within the Zoom			
CVE-2023-28601	zoom - zoom	Client. Exposure of resource to wrong sphere in Zoom for Windows and Zoom for MacOS clients before 5.14.10 may allow an	2023-06-13	6.5	Medium
CVE-2023-34114	zoom - multiple products	authenticated user to potentially enable information disclosure via network access.	2023-06-13	6.5	Medium
CVE-2023-24938	microsoft - multiple products	Windows CryptoAPI Denial of Service Vulnerability	2023-06-14	6.5	Medium
CVE-2023-29352	microsoft - multiple products	Windows Remote Desktop Security Feature Bypass Vulnerability	2023-06-14	6.5	Medium
CVE-2023-29369	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-06-14	6.5	Medium
CVE-2023-32032	microsoft - multiple products	.NET and Visual Studio Elevation of Privilege Vulnerability	2023-06-14	6.5	Medium
CVE-2023-33129 CVE-2023-33140	microsoft - multiple products microsoft - onenote	Microsoft SharePoint Denial of Service Vulnerability Microsoft OneNote Spoofing Vulnerability	2023-06-14 2023-06-14	6.5 6.5	Medium Medium
CVE-2023-33142	microsoft - multiple products	Microsoft SharePoint Server Elevation of Privilege Vulnerability	2023-06-14	6.5	Medium
CVE-2023-33145	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-06-14	6.5	Medium
CVE-2023-24937	microsoft - multiple products	Windows CryptoAPI Denial of Service Vulnerability Allocation of Resources Without Limits or Throttling vulnerability in Apache Software Foundation Apache Struts. This issue affects Apache Struts: through 2.5.30, through 6.1.2.	2023-06-14	6.5	Medium
CVE-2023-34149	apache - multiple products	Upgrade to Struts 2.5.31 or 6.1.2.1 or greater.	2023-06-14	6.5	Medium
CVE-2023-35147	jenkins - aws_codecommit_t rigger	Jenkins AWS CodeCommit Trigger Plugin 3.0.12 and earlier does not restrict the AWS SQS queue name path parameter in an HTTP endpoint, allowing attackers with Item/Read permission to obtain the contents of arbitrary files on the Jenkins controller file system.	2023-06-14	6.5	Medium
CVE-2023-35149	jenkins - digital.ai_app_man agement_publisher	A missing permission check in Jenkins Digital.ai App Management Publisher Plugin 2.6 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL, capturing credentials stored in Jenkins.	2023-06-14	6.5	Medium
CVE-2022-33159	ibm - security_directory_ suite_va	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 228567.	2023-06-15	6.5	Medium
CVE-2023-29289	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an XML Injection vulnerability. An attacker with low privileges can trigger a specially crafted script to a security feature bypass. Exploitation of this issue does not require user interaction.	2023-06-15	6.5	Medium
CVE-2023-33306	fortinet - multiple products	A null pointer dereference in Fortinet FortiOS before 7.2.5, before 7.0.11 and before 6.4.13, FortiProxy before 7.2.4 and before 7.0.10 allows attacker to denial of sslvpn service via specifically crafted request in bookmark parameter.	2023-06-16	6.5	Medium
<u> </u>	fortinet - multiple	A null pointer dereference in Fortinet FortiOS before 7.2.5 and before 7.0.11, FortiProxy before 7.2.3 and before 7.0.9 allows attacker to denial of sslvpn service via specifically crafted request	2023-00-10	0.5	Mediall
CVE-2023-33307	products microsoft - multiple	in network parameter.	2023-06-16	6.5	Medium
CVE-2023-33132	products	Microsoft SharePoint Server Spoofing Vulnerability SAP NetWeaver Enterprise Portal - version 7.50, does not sufficiently encode user-controlled inputs over the network, resulting in reflected Cross-Site Scripting (XSS) vulnerability, therefore changing the scope of the attack. On successful	2023-06-14	6.3	Medium
CVE-2023-33985	sap - netweaver	therefore changing the scope of the attack. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	2023-06-13	6.1	Medium
	sap - customer_relations hip_management_	SAP CRM ABAP (Grantor Management) - versions 700, 701, 702, 712, 713, 714, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can cause limited impact on	- 2 30 10		2
CVE-2023-33986	abap microfocus -	confidentiality and integrity of the application. Potential Cross-Site Scripting in ArcSight Logger versions prior to	2023-06-13	6.1	Medium
CVE-2023-24469	arcsight_logger	7.3.0 Open redirect vulnerability in the Layout module's SEO configuration in Liferay Portal 7.4.3.70 through 7.4.3.76, and	2023-06-13	6.1	Medium
CVE-2023-35029	liferay - multiple products	Liferay DXP 7.4 update 70 through 76 allows remote attackers to redirect users to arbitrary external URLs via the	2023-06-15	6.1	Medium

		`_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_ba			
		ckURL` parameter.			
		Cross-site scripting (XSS) vulnerability in the Layout module's SEO			
		configuration in Liferay Portal 7.4.3.70 through 7.4.3.73, and			
		Liferay DXP 7.4 update 70 through 73 allows remote attackers to			
	liferay - multiple	inject arbitrary web script or HTML via the `_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_ba			
CVE-2023-3193	products	ckURL` parameter.	2023-06-15	6.1	Mediur
	microsoft - multiple	p			
CVE-2023-32020	products	Windows DNS Spoofing Vulnerability	2023-06-14	5.6	Mediur
		A flaw was found in the Framebuffer Console (fbcon) in the Linux			
		Kernel. When providing font->width and font->height greater than			
	linux - multiple	32 to fbcon_set_font, since there are no checks in place, a shift- out-of-bounds occurs leading to undefined behavior and possible			
CVE-2023-3161	products	denial of service.	2023-06-12	5.5	Mediur
	ртович	An incorrect default permission [CWE-276] vulnerability in			
		FortiClient (Windows) versions 7.0.0 through 7.0.6 and 6.4.0			
		through 6.4.8 and FortiConverter (Windows) versions 6.2.0			
		through 6.2.1, 7.0.0 and all versions of 6.0.0 may allow a local			
	fortingt multiple	authenticated attacker to tamper with files in the installation			
CVE-2022-33877	fortinet - multiple products	folder, if FortiClient or FortiConverter is installed in an insecure folder.	2023-06-13	5.5	Mediun
CVL-2022-33877	microsoft - multiple	Tolder.	2023-00-13	3.3	Median
CVE-2023-21569	products	Azure DevOps Server Spoofing Vulnerability	2023-06-14	5.5	Mediun
	microsoft - multiple	Sysinternals Process Monitor for Windows Denial of Service			
CVE-2023-29353	products	Vulnerability	2023-06-14	5.5	Mediun
	microsoft - multiple				
CVE-2023-32016	products	Windows Installer Information Disclosure Vulnerability	2023-06-14	5.5	Mediun
	microsoft - multiple				
CVE-2023-33139	products	Visual Studio Information Disclosure Vulnerability	2023-06-14	5.5	Mediun
		An improper authorization check of local device settings in TeamViewer Remote between version 15.41 and 15.42.7 for			
		Windows and macOS allows an unprivileged user to change basic			
	teamviewer -	local device settings even though the options were locked. This			
CVE-2023-0837	remote	can result in unwanted changes to the configuration.	2023-06-14	5.5	Mediun
		In multiple functions of ChooserActivity.java, there is a possible			
		cross-user media read due to a confused deputy. This could lead to			
		local information disclosure with no additional execution privileges			
	1 100 1	needed. User interaction is not needed for exploitation.Product:			
CVE 2022 2110E	google - multiple	AndroidVersions: Android-11 Android-12 Android-12L Android-	2022 06 15		Mediun
CVE-2023-21105	products	13Android ID: A-261036568 In multiple functions of JobStore.java, there is a possible way to	2023-06-15	5.5	iviediun
		cause a crash on startup due to improper input validation. This			
		could lead to local denial of service with no additional execution			
		privileges needed. User interaction is not needed for			
	google - multiple	exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2023-21136	products	Android-12L Android-13Android ID: A-246542285	2023-06-15	5.5	Mediun
		In several methods of JobStore.java, uncaught exceptions in job			
		map parsing could lead to local persistent denial of service with no			
	google - multiple	additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11			
CVE-2023-21137	products	Android-12 Android-12L Android-13Android ID: A-246541702	2023-06-15	5.5	Mediun
CVE ZOZS ZIISI	products	In several functions of several files, there is a possible way to	2023 00 13	3.3	Wicaran
		access developer mode traces due to a permissions bypass. This			
		could lead to local information disclosure with no additional			
		execution privileges needed. User interaction is not needed for			
	google - multiple	exploitation.Product: AndroidVersions: Android-11 Android-12			
CVE-2023-21141	products	Android-12L Android-13Android ID: A-262244249	2023-06-15	5.5	Mediun
		In multiple files, there is a possible way to access traces in the dev			
		mode due to a permissions bypass. This could lead to local			
		information disclosure with no additional execution privileges			
		information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation Product:			
	google - multiple	information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-			
CVE-2023-21142	google - multiple products	needed. User interaction is not needed for exploitation.Product:	2023-06-15	5.5	Mediur
CVE-2023-21142		needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-	2023-06-15	5.5	Mediun
CVE-2023-21142		needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665	2023-06-15	5.5	Mediur
CVE-2023-21142		needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution	2023-06-15	5.5	Mediur
CVE-2023-21142	products	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for	2023-06-15	5.5	Mediur
	products google - multiple	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12			
	products	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777	2023-06-15	5.5	
	products google - multiple	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777 SAP NetWeaver (Design Time Repository) - version 7.50, returns an			
	products google - multiple	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777 SAP NetWeaver (Design Time Repository) - version 7.50, returns an unfavorable content type for some versioned files, which could			
	products google - multiple	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777 SAP NetWeaver (Design Time Repository) - version 7.50, returns an unfavorable content type for some versioned files, which could allow an authorized attacker to create a file with a malicious			
CVE-2023-21142 CVE-2023-21143	products google - multiple	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777 SAP NetWeaver (Design Time Repository) - version 7.50, returns an unfavorable content type for some versioned files, which could			Mediun
	products google - multiple	needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android- 13Android ID: A-262243665 In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777 SAP NetWeaver (Design Time Repository) - version 7.50, returns an unfavorable content type for some versioned files, which could allow an authorized attacker to create a file with a malicious content and send a link to a victim in an email or instant message.			

		delete/replace Zoom Client files potentially causing a loss of			
		integrity and availability to the Zoom Client. Jenkins Maven Repository Server Plugin 1.10 and earlier does not			
		escape the versions of build artifacts on the Build Artifacts As			
	jenkins -	Maven Repository page, resulting in a stored cross-site scripting			
CVE-2023-35143	maven_repository_ server	(XSS) vulnerability exploitable by attackers able to control maven project versions in 'pom.xml'.	2023-06-14	5.4	Medium
CVL 2023 33143	SCIVEI	Jenkins Maven Repository Server Plugin 1.10 and earlier does not	2023 00 14	3.4	Wicalaili
	jenkins -	escape project and build display names on the Build Artifacts As			
CVE 2022 254.44	maven_repository_	Maven Repository page, resulting in a stored cross-site scripting	2022 05 44	F 4	Na di di
CVE-2023-35144	server	(XSS) vulnerability. Jenkins Sonargraph Integration Plugin 5.0.1 and earlier does not	2023-06-14	5.4	Medium
		escape the file path and the project name for the Log file field			
	jenkins -	form validation, resulting in a stored cross-site scripting			
CVE-2023-35145	sonargraph_integra tion	vulnerability exploitable by attackers with Item/Configure permission.	2023-06-14	5.4	Medium
<u> </u>	0.0	Jenkins Template Workflows Plugin 41.v32d86a_313b_4a and			
	jenkins -	earlier does not escape names of jobs used as buildings blocks for			
CVE-2023-35146	template_workflow s	Template Workflow Job, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create jobs.	2023-06-14	5.4	Medium
CVL 2023 33140	3	A reflected cross-site scripting (XSS) vulnerability in the Captive	2023 00 14	3.4	Wicaranii
		Portal feature of Palo Alto Networks PAN-OS software can allow a			
	nalaaltanatuuarka	JavaScript payload to be executed in the context of an			
CVE-2023-0010	paloaltonetworks - multiple products	authenticated Captive Portal user's browser when they click on a specifically crafted link.	2023-06-14	5.4	Medium
	, ,	Adobe Experience Manager versions 6.5.16.0 (and earlier) is			
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
	adobe - multiple	low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-29302	products	be executed within the context of the victim's browser.	2023-06-15	5.4	Medium
		Adobe Experience Manager versions 6.5.16.0 (and earlier) is			
		affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL			
	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may			
CVE-2023-29304	products	be executed within the context of the victim's browser.	2023-06-15	5.4	Medium
		Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a URL Redirection to Untrusted Site ('Open Redirect')			
		vulnerability. A low-privilege authenticated attacker could			
	adobe - multiple	leverage this vulnerability to redirect users to malicious websites.			
CVE-2023-29307	products	Exploitation of this issue requires user interaction.	2023-06-15	5.4	Medium
		Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a			
		low-privileged attacker is able to convince a victim to visit a URL			
CVE 2022 20222	adobe - multiple	referencing a vulnerable page, malicious JavaScript content may	2022 06 15	г 4	Madium
CVE-2023-29322	products microsoft - multiple	be executed within the context of the victim's browser.	2023-06-15	5.4	Medium
CVE-2023-29355	products	DHCP Server Service Information Disclosure Vulnerability	2023-06-14	5.3	Medium
0.45 0.000 0.004.0	microsoft - multiple		2022 05 44		
CVE-2023-32013	products	Windows Hyper-V Denial of Service Vulnerability Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and	2023-06-14	5.3	Medium
		earlier) and 2.4.4-p3 (and earlier) are affected by an Information			
		Exposure vulnerability that could lead to a security feature bypass.			
CVE-2023-29287	adobe - multiple products	An attacker could leverage this vulnerability to leak minor user data. Exploitation of this issue does not require user interaction	2023-06-15	5.3	Medium
541 2025 ZJ201	products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and	-023 00-13	٠.٥	ivicululli
		earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect			
		Authorization vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to bypass a			
	adobe - multiple	minor functionality. Exploitation of this issue does not require user			
CVE-2023-29290	products	interaction.	2023-06-15	5.3	Medium
		Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and			
		earlier) and 2.4.4-p3 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary			
		file system read. An admin-privilege authenticated attacker can			
		force the application to make arbitrary requests via injection of			
CVE-2023-29291	adobe - multiple products	arbitrary URLs. Exploitation of this issue does not require user interaction.	2023-06-15	4.9	Medium
<u> </u>	p. 044613	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and	_023 00 13		caiaiii
		earlier) and 2.4.4-p3 (and earlier) are affected by a Server-Side			
		Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. An admin-privilege authenticated 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-2023-29292	products	interaction.	2023-06-15	4.9	Medium
		An improper certificate validation vulnerability [CWE-295] in FortiOS 6.2 all versions, 6.4 all versions, 7.0.0 through 7.0.10, 7.2.0			
		and FortiProxy 1.2 all versions, 2.0 all versions, 7.0.0 through 7.0.9,			
0/5 0000 000	fortinet - multiple	7.2.0 through 7.2.3 may allow a remote and unauthenticated	2022 25 55		
CVE-2023-29175	products	attacker to perform a Man-in-the-Middle attack on the	2023-06-13	4.8	Medium

		communication channel between the vulnerable device and the remote FortiGuard's map server.			
CVE 2022 22010	microsoft - multiple	Windows Kernel Information Disclosure Vulnerability	2023-06-14	47	Madium
CVE-2023-32019	products	Windows Kernel Information Disclosure Vulnerability In canStartSystemGesture of RecentsAnimationDeviceState.java,	2023-06-14	4.7	Medium
		there is a possible partial lockscreen bypass due to a race			
		condition. This could lead to local escalation of privilege with no			
	google - multiple	additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L			
CVE-2023-21095	products	Android-13Android ID: A-242704576	2023-06-15	4.7	Medium
		A cleartext transmission of sensitive information vulnerability			
		[CWE-319] in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.8, FortiProxy version 7.2.0 through 7.2.1 and 7.0.0			
		through 7.0.8 allows an authenticated attacker with readonly			
	fortinet - multiple	superadmin privileges to intercept traffic in order to obtain other			
CVE-2022-41327	products	adminstrators cookies via diagnose CLI commands. A access of uninitialized pointer vulnerability [CWE-824] in	2023-06-13	4.4	Medium
		Fortinet FortiProxy version 7.2.0 through 7.2.3 and before 7.0.9			
		and FortiOS version 7.2.0 through 7.2.4 and before 7.0.11 allows			
CVE 2022 20470	fortinet - multiple	an authenticated attacker to repetitively crash the httpsd process	2022 06 42	4.2	N.A. adiia
CVE-2023-29178	products	via crafted HTTP or HTTPS requests. Zoom clients prior to 5.13.10 contain an HTML injection	2023-06-13	4.3	Medium
		vulnerability. A malicious user could inject HTML into their display			
	zoom - multiple	name potentially leading a victim to a malicious website during			
CVE-2023-28599	products	meeting creation. Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and	2023-06-13	4.3	Medium
		earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect			
		Authorization vulnerability that could result in a security feature			
	adobe - multiple	bypass. A privileged attacker could leverage this vulnerability to modify a minor functionality of another user's data. Exploitation of			
CVE-2023-29288	products	this issue does not require user interaction.	2023-06-15	4.3	Medium
	į i i i i i i i i i i i i i i i i i i i	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and			
		earlier) and 2.4.4-p3 (and earlier) are affected by a Business Logic			
		Errors vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass			
	adobe - multiple	a minor functionality. Exploitation of this issue does not require			
CVE-2023-29294	products	user interaction.	2023-06-15	4.3	Medium
		Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect			
		Authorization vulnerability that could result in a security feature			
		bypass. A low-privileged attacker could leverage this vulnerability			
CVE 2022 2020E	adobe - multiple	to bypass a minor functionality. Exploitation of this issue does not	2022 06 45	4.2	N 4 o diviso
CVE-2023-29295	products	require user interaction. Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and	2023-06-15	4.3	Medium
		earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect			
		Authorization vulnerability that could result in a security feature			
	adobe - multiple	bypass. A low-privileged attacker could leverage this vulnerability to modify a minor functionality of another user's data. Exploitation			
CVE-2023-29296	products	of this issue does not require user interaction.	2023-06-15	4.3	Medium
		A fully compromised ESXi host can force VMware Tools to fail to			
CVE-2023-20867	vmware - tools	authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine.	2023-06-13	3.9	Low
<u> </u>	Timure tools	Buffer copy without checking size of input in Zoom Meeting SDK	2020 00 10	0.5	2011
		before 5.13.0 may allow an authenticated user to potentially			
CVE-2023-34115	zoom - meeting_sdk	enable a denial of service via local access. This issue may result in the Zoom Meeting SDK to crash and need to be restarted.	2023-06-13	3.8	Low
<u>5.2 2525 57115</u>	microsoft - multiple		_023 00 13	3.0	
CVE-2023-28303	products	Windows Snipping Tool Information Disclosure Vulnerability	2023-06-13	3.3	Low
CVE-2023-32024	microsoft -	Microsoft Power Apps Spoofing Vulnerability	2023-06-14	3	Low
CVL-2023-32024	power_apps	SAP NetWeaver (Change and Transport System) - versions 702,	202J-00-14	J	LUVV
		731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an			
		authenticated user with admin privileges to maliciously run a			
		benchmark program repeatedly in intent to slowdown or make the server unavailable which may lead to a limited impact on			
	sap - multiple	Availability with No impact on Confidentiality and Integrity of the			
CVE-2023-32114	products	application.	2023-06-13	2.7	Low
		A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9 and before			
		6.4.12, FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through			
	formation at 111 1	7.0.7, FortiSwitchManager version 7.2.0 through 7.2.1 and before			
CVE-2022-42474	fortinet - multiple products	7.0.1 allows an privileged attacker to delete arbitrary directories from the filesystem through crafted HTTP requests.	2023-06-13	2.7	Low
	p. 55.55	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and			
		earlier) and 2.4.4-p3 (and earlier) are affected by an Improper			
		Input Validation vulnerability that could result in a Security feature bypass. An admin privileged attacker could leverage this			
	adobe - multiple	vulnerability to impact the availability of a user's minor feature.			
CVE-2023-29293	products	Exploitation of this issue does not require user interaction.	2023-06-15	2.7	Low

Where NCA provides the vulnerability information as published by NIST's وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.