

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

خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني للمساعدة في حماية الفضاء السيبراني protecting national interests, NCA provides the weekly summary of the National الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل published vulnerabilities by the National Institute of Standards and Institute of Standards and Technology (NIST) National Technology (NIST) National Vulnerability Database (NVD) for the للأسبوع من ٦ أغسطس إلى ١٢ أغسطس علماً Vulnerability Database (NVD) week from 6th of August to 12th of August. Vulnerabilities are scored Common Vulnerability Scoring اُنه يتم تُصنيف هذه الثغراُت باستخدام معيار 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

System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

عالى جدًا: النتيجة الأساسية لـ10.0-CVSS 9.0-10.0

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 &	Vendor - Product	Description	Publish Date	CVS S	Severity
Source	Torract Troduct	2 costipation	, asiisii sate	Score	Governy
		Netgear R7100LG 1.0.0.78 was discovered to contain a command			
	netgear -	injection vulnerability via the password parameter at			
CVE-2023-38928	r7100lg_firmware	usb_remote_invite.cgi.	2023-08-07	9.8	Critical
		SAP PowerDesigner - version 16.7, has improper access control			
	sap -	which might allow an unauthenticated attacker to run arbitrary			
CVE-2023-37483	powerdesigner	queries against the back-end database via Proxy.	2023-08-08	9.8	Critical
		SAP Commerce Cloud may accept an empty passphrase for user ID			
	sap - multiple	and passphrase authentication, allowing users to log into the			
CVE-2023-39439	products	system without a passphrase.	2023-08-08	9.8	Critical
	qualcomm -	Memory corruption due to buffer copy without checking size of			_
<u>CVE-2022-40510</u>	apq8009_firmware	input in Audio while voice call with EVS vocoder.	2023-08-08	9.8	Critical
		A vulnerability has been identified in RUGGEDCOM i800,			
		RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC,			
		RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803,			
		RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM			
		M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200,			
		RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM			
		M969, RUGGEDCOM M969F, RUGGEDCOM M969NC,			
		RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM			
		RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM			
		RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM			
		RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600, RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM			
		RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC,			
		RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM			
		RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC,			
		RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM			
		RS416NC, RUGGEDCOM RS416NC v2, RUGGEDCOM RS416P,			
		RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM			
		RS416PNC v2, RUGGEDCOM RS416Pv2, RUGGEDCOM RS416v2,			
		RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM			
		RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC,			
		RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM			
		RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900,			
		RUGGEDCOM RS900 (32M) V4.X, RUGGEDCOM RS900 (32M) V5.X,			
		RUGGEDCOM RS900F, RUGGEDCOM RS900G, RUGGEDCOM			
		RS900G (32M) V4.X, RUGGEDCOM RS900G (32M) V5.X,			
		RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM			
		RS900GNC(32M) V4.X, RUGGEDCOM RS900GNC(32M) V5.X,			
		RUGGEDCOM RS900GP, RUGGEDCOM RS900GPF, RUGGEDCOM			
		RS900GPNC, RUGGEDCOM RS900L, RUGGEDCOM RS900L,			
		RUGGEDCOM RS900LNC, RUGGEDCOM RS900LNC, RUGGEDCOM			
		RS900M-GETS-C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM			
		RS900M-STND-C01, RUGGEDCOM RS900M-STND-XX,			
		RUGGEDCOM RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-			
		GETS-XX, RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM			
		RS900MNC-STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM			
	siemens -	RS900NC, RUGGEDCOM RS900NC(32M) V4.X, RUGGEDCOM			
CVE-2023-24845	ruggedcom_ros	RS900NC(32M) V5.X, RUGGEDCOM RS900W, RUGGEDCOM RS910,	2023-08-08	9.8	Critical

		RUGGEDCOM RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC, RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L, RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC, RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200, RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PV4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2300PV4.X, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG240PNC V5.X, RUGGEDCOM RSG2488 V4.X, RUGGEDCOM RSG240PNC V5.X, RUGGEDCOM RSG290PNC V4.X, RUGGEDCOM RSG90PNC V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM RSG920PNC V4.X, RUGGEDC			
	qualcomm -	An attacker could use this behavior to transmit malicious packets to systems in the mirrored network, possibly influencing their configuration and runtime behavior.  Memory corruption in QESL while processing payload from			
CVE-2023-28561	qcn7606_firmware  siemens - ruggedcom_crossb	external ESL device to firmware.  A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an unauthenticated remote attackers to	2023-08-08	9.8	Critical
CVE-2023-37372	ow	execute arbitrary SQL queries on the server database.	2023-08-08	9.8	Critical
CVE-2023-21709	microsoft - multiple products	Microsoft Exchange Server Elevation of Privilege Vulnerability	2023-08-08	9.8	Critical
CVE-2023-35385	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability  Path traversal in Zoom Desktop Client for Windows before 5.14.7	2023-08-08	9.8	Critical
CVE-2023-36534	zoom - zoom	may allow an unauthenticated user to enable an escalation of privilege via network access.	2023-08-08	9.8	Critical
CVE-2023-36903	microsoft - multiple products	Windows System Assessment Tool Elevation of Privilege Vulnerability	2023-08-08	9.8	Critical
CVE-2023-36910	microsoft - multiple products	Microsoft Message Queuing Remote Code Execution Vulnerability	2023-08-08	9.8	Critical
CVE-2023-36911	microsoft - multiple products microsoft - multiple	Microsoft Message Queuing Remote Code Execution Vulnerability Windows Mobile Device Management Elevation of Privilege	2023-08-08	9.8	Critical
CVE-2023-38186	products	Vulnerability Improper input validation in Zoom Desktop Client for Windows	2023-08-08	9.8	Critical
CVE-2023-39216	zoom - zoom	before 5.14.7 may allow an unauthenticated user to enable an escalation of privilege via network access.	2023-08-08	9.8	Critical
CVE-2023-39213	zoom - multiple products	Improper neutralization of special elements in Zoom Desktop Client for Windows and Zoom VDI Client before 5.15.2 may allow an unauthenticated user to enable an escalation of privilege via network access.	2023-08-08	9.8	Critical
CAT-5072-22712	·	Out-of-bounds write vulnerability in parser_hvcC function of	2023-00-Uŏ	3.0	Cittical
CVE-2023-30699	samsung - multiple products	libsimba library prior to SMR Aug-2023 Release 1 allows code execution by remote attackers.  Ivanti Avalanche decodeToMap XML External Entity Processing.	2023-08-10	9.8	Critical
CVE-2023-32567	ivanti - avalanche	Fixed in version 6.4.1.  An attacker can send a specially crafted message to the Wavelink	2023-08-10	9.8	Critical
		Avalanche Manager, which could result in service disruption or arbitrary code execution.			
		Thanks to a Researcher at Tenable for finding and reporting.			
CVE-2023-32560	ivanti - avalanche	Fixed in version 6.4.1.  An unrestricted upload of file with dangerous type vulnerability	2023-08-10	9.8	Critical
CVE-2023-32562	ivanti - avalanche	exists in Avalanche versions 6.3.x and below that could allow an	2023-08-10	9.8	Critical

		attacker to achieve a remove code execution. Fixed in version 6.4.1.			
		An unauthenticated attacker could achieve the code execution			_
CVE-2023-32563	ivanti - avalanche	through a RemoteControl server.  An unrestricted upload of file with dangerous type vulnerability	2023-08-10	9.8	Critical
		exists in Avalanche versions 6.4.1 and below that could allow an			
CVE-2023-32564	ivanti - avalanche	attacker to achieve a remove code execution.	2023-08-10	9.8	Critical
	intel -	Improper access control in the Intel(R) Ethernet Controller RDMA			
	ethernet_controller	driver for linux before version 1.9.30 may allow an			
0.45 0000 05555	_rdma_driver_for_l	unauthenticated user to potentially enable escalation of privilege			
CVE-2023-25775	inux	via network access.	2023-08-11	9.8	Critical
		A vulnerability was discovered in Veritas NetBackup Snapshot Manager before 10.2.0.1 that allowed untrusted clients to interact			
		with the RabbitMQ service. This was caused by improper			
		validation of the client certificate due to misconfiguration of the			
		RabbitMQ service. Exploiting this impacts the confidentiality and			
		integrity of messages controlling the backup and restore jobs, and			
		could result in the service becoming unavailable. This impacts only the jobs controlling the backup and restore activities, and does not			
		allow access to (or deletion of) the backup snapshot data itself.			
		This vulnerability is confined to the NetBackup Snapshot Manager			
	veritas - multiple	feature and does not impact the RabbitMQ instance on the			
CVE-2023-40256	products	NetBackup primary servers.	2023-08-11	9.8	Critical
	tar d	Cross-site Scripting (XSS) in some Intel(R) Manageability			
	intel - manageability_com	Commander software before version 2.3 may allow an unauthenticated user to potentially enable escalation of privilege			
CVE-2022-29887	manageability_com mander	via network access.	2023-08-11	9.6	Critical
<u> </u>	intel -	Cross-site scripting (XSS) for the Intel(R) DSA software before	2023 00 11	3.0	Critical
	driver_\&_support	version 23.1.9 may allow unauthenticated user to potentially			
CVE-2023-27515	_assistant	enable escalation of privilege via network access.	2023-08-11	9.6	Critical
		Improper Input Validation vulnerability in Apache Software			
CVE 2022 22024	apache - multiple	Foundation Apache Traffic Server. This issue affects Apache Traffic	2023-08-09	0.1	Critical
CVE-2023-33934	products	Server: through 9.2.1.  An attacker can send a specially crafted request which could lead	2023-08-09	9.1	Critical
		to leakage of sensitive data or potentially a resource-based DoS			
CVE-2023-32566	ivanti - avalanche	attack. Fixed in version 6.4.1.	2023-08-10	9.1	Critical
		An attacker can send a specially crafted request which could lead			
		to leakage of sensitive data or potentially a resource-based DoS			
CVE-2023-32565	ivanti - avalanche	attack. Fixed in version 6.4.1.	2023-08-10	9.1	Critical
		SAP Business Objects Installer - versions 420, 430, allows an authenticated attacker within the network to overwrite an			
		executable file created in a temporary directory during the			
		installation process. On replacing this executable with a malicious			
	sap - multiple	file, an attacker can completely compromise the confidentiality,			
CVE-2023-37490	products	integrity, and availability of the system	2023-08-08	9	Critical
		Netgear XR300 v1.0.3.78 was discovered to contain multiple buffer			
CVE-2023-36499	netgear - xr300_firmware	overflows via the wla_ssid and wlg_ssid parameters at genie_ap_wifi_change.cgi.	2023-08-07	8.8	High
<u>CVL 2023 30 133</u>	xi300_iiiiiwaic	Netgear R6900P v1.3.3.154 was discovered to contain multiple	2023 00 07	0.0	111611
	netgear -	buffer overflows via the wla_ssid and wlg_ssid parameters at			
CVE-2023-38412	r6900p_firmware	ia_ap_setting.cgi.	2023-08-07	8.8	High
	netgear -	Netgear DG834Gv5 1.6.01.34 was discovered to contain multiple			
CVE-2023-38591	dg834gv5_firmwar	buffer overflows via the wla_ssid and wla_temp_ssid parameters at bsw_ssid.cgi.	2023-08-07	8.8	High
CAF-5052-20221	e	Netgear WG302v2 v5.2.9 and WAG302v2 v5.1.19 were discovered	2023-06-07	0.0	nigii
		to contain multiple command injection vulnerabilities in the			
	netgear -	upgrade_handler function via the firmwareRestore and			
CVE-2023-38921	wg302v2_firmware	firmwareServerip parameters.	2023-08-07	8.8	High
	_	Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and			
	netgear - jwnr2000v2_firmw	XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in			
CVE-2023-38922	are	the update auth function.	2023-08-07	8.8	High
<u> </u>	u.c	Netgear DC112A 1.0.0.64, EX6200 1.0.3.94 and R6300v2 1.0.4.8		0.0	6'''
		were discovered to contain a buffer overflow via the http_passwd			
	netgear -	were discovered to contain a barrer overmon via the http_passiva		l .	
CVE-2023-38925	netgear - dc112a_firmware	parameter in password.cgi.	2023-08-07	8.8	High
CVE-2023-38925	dc112a_firmware	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer	2023-08-07	8.8	High
	dc112a_firmware netgear -	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at			_
CVE-2023-38925  CVE-2023-38926	dc112a_firmware	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.	2023-08-07	8.8	High High
	dc112a_firmware netgear -	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at			_
	dc112a_firmware  netgear - ex6200_firmware	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.  Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and			
	netgear - ex6200_firmware  netgear -	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.  Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function.			
CVE-2023-38926	netgear - ex6200_firmware  netgear - jwnr2000v2_firmw	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.  Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function.  The ACL (Access Control List) of SAP Message Server - versions	2023-08-07	8.8	High
CVE-2023-38926	netgear - ex6200_firmware  netgear - jwnr2000v2_firmw	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.  Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function.  The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC	2023-08-07	8.8	High
CVE-2023-38926	netgear - ex6200_firmware  netgear - jwnr2000v2_firmw	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.  Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function.  The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22,	2023-08-07	8.8	High
CVE-2023-38926	netgear - ex6200_firmware  netgear - jwnr2000v2_firmw	parameter in password.cgi.  Netgear EX6200 v1.0.3.94 was discovered to contain a buffer overflow via the wla_temp_ssid parameter at acosNvramConfig_set.  Netgear JWNR2000v2 v1.0.0.11, XWN5001 v0.4.1.1, and XAVN2001v2 v0.4.0.7 were discovered to contain multiple buffer overflows via the http_passwd and http_username parameters in the check_auth function.  The ACL (Access Control List) of SAP Message Server - versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC	2023-08-07	8.8	High

		This may lead to unauthorized read and write of data as well as			
		rendering the system unavailable.			
		A vulnerability has been identified in RUGGEDCOM CROSSBOW (All			
	siemens -	versions < V5.4). The affected applications is vulnerable to SQL injection. This could allow an authenticated remote attackers to			
VE-2023-27411	ruggedcom_crossb ow	execute arbitrary SQL queries on the server database and escalate privileges.	2023-08-08	8.8	High
VE 2023 27411	microsoft - multiple	privileges.	2023 00 00	0.0	11161
VE-2023-29328	products	Microsoft Teams Remote Code Execution Vulnerability	2023-08-08	8.8	High
	microsoft - multiple	,			
VE-2023-29330	products	Microsoft Teams Remote Code Execution Vulnerability	2023-08-08	8.8	High
	microsoft - multiple	·			
VE-2023-35368	products	Microsoft Exchange Remote Code Execution Vulnerability	2023-08-08	8.8	High
	microsoft - multiple				
VE-2023-35381	products	Windows Fax Service Remote Code Execution Vulnerability	2023-08-08	8.8	High
	microsoft - multiple	Windows Bluetooth A2DP driver Elevation of Privilege			
VE-2023-35387	products	Vulnerability	2023-08-08	8.8	High
		Insufficient verification of data authenticity in Zoom Desktop			
		Client for Windows before 5.14.5 may allow an authenticated user			
VE-2023-36541	zoom - zoom	to enable an escalation of privilege via network access.	2023-08-08	8.8	High
	microsoft - multiple	Microsoft WDAC OLE DB provider for SQL Server Remote Code			
/E-2023-36882	products	Execution Vulnerability	2023-08-08	8.8	Higl
	microsoft - multiple				
/E-2023-38169	products	Microsoft OLE DB Remote Code Execution Vulnerability	2023-08-08	8.8	High
	microsoft - multiple				
VE-2023-38181	products	Microsoft Exchange Server Spoofing Vulnerability	2023-08-08	8.8	Higl
	microsoft - multiple				
VE-2023-38185	products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-08-08	8.8	High
	microsoft -			_	
VE-2023-36899	.net_framework	ASP.NET Elevation of Privilege Vulnerability	2023-08-08	8.8	Higl
		Uncontrolled search path for the Intel(R) Al Hackathon software			
		before version 2.0.0 may allow an unauthenticated user to	0000 55		
VE-2023-28380	intel - ai_hackathon	potentially enable escalation of privilege via network access.	2023-08-11	8.8	High
		Exposure of sensitive information in Zoom Client SDK's before			
VE 2225 555	zoom - multiple	5.15.5 may allow an authenticated user to enable a denial of	2000 5		
VE-2023-39214	products	service via network access.	2023-08-08	8.1	Higl
VE 2225 5==	microsoft - multiple		2000 5	_	
VE-2023-35388	products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-08-08	8	Higl
	microsoft - multiple		0.555	_	
VE-2023-36891	products	Microsoft SharePoint Server Spoofing Vulnerability	2023-08-08	8	High
VE 2022 2225	microsoft - multiple	Missassift Characteristics and Co. Co. M. J. 1999	2022 22 27		
VE-2023-36892	products	Microsoft SharePoint Server Spoofing Vulnerability	2023-08-08	8	High
VE 2022 20122	microsoft - multiple	Microsoft Fuebours Course Provide Code 5	2022 02 02		,
VE-2023-38182	products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-08-08	8	High
	intel -	Improper input validation in the BIOS firmware for some Intel(R)			
VE 2022 44644	celeron_j6413_firm	Processors may allow a privileged user to potentially enable	2022 00 44	c	11:-1
VE-2022-44611	ware	escalation of privilege via adjacent access.	2023-08-11	8	High
		A use-after-free flaw was found in the Linux kernel's Netfilter			
	linuv multinla	functionality when adding a rule with NFTA_RULE_CHAIN_ID. This			
VF_2022 4147	linux - multiple products	flaw allows a local user to crash or escalate their privileges on the	2023-08-07	7.8	ام: ال
CVE-2023-4147	products	system.  SAP SQLA for PowerDesigner 17 bundled with SAP PowerDesigner	ZUZ3-Uð-U/	7.8	Higl
		16.7 SP06 PL03, allows an attacker with local access to the system,			
		to place a malicious library, that can be executed by the			
	sap -	application. An attacker could thereby control the behavior of the			
VE-2023-36923	powerdesigner	application. An attacker could thereby control the behavior of the application.	2023-08-08	7.8	Higl
	POWELGESIGNE	A vulnerability has been identified in Siemens Software Center (All	2020 00-00	, .0	ı ııgı
		versions < V3.0). A DLL Hijacking vulnerability could allow a local			
	siemens -	attacker to execute code with elevated privileges by placing a			
VE-2021-41544	software_center	malicious DLL in one of the directories on the DLL search path.	2023-08-08	7.8	Higl
		A vulnerability has been identified in SICAM TOOLBOX II (All		0	6
		versions < V07.10). Affected applications do not properly set			
		permissions for product folders. This could allow an authenticated			
	siemens -	attacker with low privileges to replace DLLs and conduct a privilege			
VE-2022-39062	sicam_toolbox_ii	escalation.	2023-08-08	7.8	Hig
	qualcomm -	Memory corruption in Trusted Execution Environment while		-	.0
VE-2023-21627	aqt1000_firmware	calling service API with invalid address.	2023-08-08	7.8	Higl
	qualcomm -				<u> </u>
	apq8064au_firmwa	Memory corruption due to untrusted pointer dereference in			
VE-2023-21643	re	automotive during system call.	2023-08-08	7.8	Higl
	qualcomm -	J : /			0
VE-2023-21648	aqt1000_firmware	Memory corruption in RIL while trying to send apdu packet.	2023-08-08	7.8	Higl
	qualcomm -	, , , , , , , , , , , , , , , , , , , ,		-	0
	apq8096au_firmwa	Memory corruption in WLAN while running doDriverCmd for an			
VE-2023-21649	re	unspecific command.	2023-08-08	7.8	High
	qualcomm -	Memory Corruption in GPS HLOS Driver when injectFdclData			<u> </u>
	1	, , ,			

	qualcomm -	Memory Corruption in Core due to incorrect type conversion or			
CVE-2023-21651	aqt1000_firmware	cast in secure_io_read/write function in TEE.	2023-08-08	7.8	High
CVE-2023-22666	qualcomm - apq8009_firmware	Memory Corruption in Audio while playing amrwbplus clips with modified content.	2023-08-08	7.8	High
	qualcomm -				
CVE-2023-28537	315_5g_iot_mode m firmware	Memory corruption while allocating memory in COmxApeDec module in Audio.	2023-08-08	7.8	High
<u>CVL-2023-28337</u>	III_IIIIIIWale	The cam_get_device_priv function does not check the type of	2023-08-08	7.0	Tilgii
	qualcomm -	handle being returned (device/session/link). This would lead to			
CVE-2023-28575	aqt1000_firmware	invalid type usage if a wrong handle is passed to it.	2023-08-08	7.8	High
		In the function call related to CAM_REQ_MGR_RELEASE_BUF there is no check if the buffer is being used. So when a function			
	qualcomm -	called cam_mem_get_cpu_buf to get the kernel va to use, another			
CVE 2022 20577	fastconnect_6800_f	thread can call CAM_REQ_MGR_RELEASE_BUF to unmap the	2022 00 00	7.0	112.1
CVE-2023-28577	irmware	kernel va which cause UAF of the kernel address.  A vulnerability has been identified in JT2Go (All versions <	2023-08-08	7.8	High
		V14.2.0.5), Solid Edge SE2022 (All versions < V222.0 Update 13),			
		Solid Edge SE2023 (All versions < V223.0 Update 4), Teamcenter			
		Visualization V13.2 (All versions < V13.2.0.15), Teamcenter Visualization V13.3 (All versions < V13.3.0.11), Teamcenter			
		Visualization V14.1 (All versions < V14.1.0.11), Teamcenter			
		Visualization V14.2 (All versions < V14.2.0.5). The affected			
		application contains a use-after-free vulnerability that could be triggered while parsing specially crafted ASM file. An attacker			
	siemens - multiple	could leverage this vulnerability to execute code in the context of			
CVE-2023-28830	products	the current process.	2023-08-08	7.8	High
		A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4), Parasolid V34.0 (All			
		versions < V34.0.253), Parasolid V34.1 (All versions < V34.1.243),			
		Parasolid V35.0 (All versions < V35.0.177), Parasolid V35.1 (All			
		versions < V35.1.073). The affected applications contain an out of bounds read past the end of an allocated structure while parsing			
	siemens - multiple	specially crafted JT files. This could allow an attacker to execute			
CVE-2023-30795	products	code in the context of the current process.	2023-08-08	7.8	High
		A vulnerability has been identified in JT Open (All versions < V11.4), JT Utilities (All versions < V13.4). The affected applications			
		contain an out of bounds read past the end of an allocated			
	siemens - multiple	structure while parsing specially crafted JT files. This could allow			
CVE-2023-30796	products	an attacker to execute code in the context of the current process.  A vulnerability has been identified in Parasolid V34.1 (All versions	2023-08-08	7.8	High
		< V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid			
		V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1			
		(All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The			
		affected applications contain null pointer dereference while			
	siemens - multiple	parsing specially crafted X_T files. This could allow an attacker to			
CVE-2023-38524	products	execute code in the context of the current process.  A vulnerability has been identified in Parasolid V34.1 (All versions	2023-08-08	7.8	High
		< V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid			
		V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1			
		(All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The			
		affected applications contain an out of bounds read past the end			
		of an allocated structure while parsing specially crafted X_T files.			
CVE-2023-38525	siemens - multiple products	This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
<u> </u>	p. oddets	A vulnerability has been identified in Parasolid V34.1 (All versions	2020 00 00	, .0	111811
		< V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid			
		V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions <			
		V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The			
		affected applications contain an out of bounds read past the end			
	siemens - multiple	of an allocated structure while parsing specially crafted X_T files.  This could allow an attacker to execute code in the context of the			
CVE-2023-38526	products	current process.	2023-08-08	7.8	High
		A vulnerability has been identified in Parasolid V34.1 (All versions			
		< V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Teamcenter Visualization V14.1 (All versions), Teamcenter			
		Visualization V14.2 (All versions < V14.2.0.6), Teamcenter			
		Visualization V14.3 (All versions). The affected applications contain			
	siemens - multiple	an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to			
CVE-2023-38527	products	execute code in the context of the current process.	2023-08-08	7.8	High
		A vulnerability has been identified in Parasolid V34.1 (All versions			
		< V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions <			
		V35.1 (All versions < V35.1.197), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions),			
0.45 0.55	siemens - multiple	Teamcenter Visualization V14.2 (All versions < V14.2.0.6),			
CVE-2023-38528	products	Teamcenter Visualization V14.3 (All versions). The affected	2023-08-08	7.8	High

	T			Г	
		application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted X_T file. This could allow an attacker to execute code in the context of the			
		current process.  A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files.			
CVE-2023-38529	siemens - multiple products	This could allow an attacker to execute code in the context of the current process.	2023-08-08	7.8	High
	siemens - multiple	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the			
CVE-2023-38530	products	current process.	2023-08-08	7.8	High
	siemens - multiple	A vulnerability has been identified in Parasolid V34.1 (All versions < V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid V35.1 (All versions < V35.1.184), Teamcenter Visualization V14.1 (All versions), Teamcenter Visualization V14.2 (All versions < V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the			
CVE-2023-38531	products	current process.	2023-08-08	7.8	High
		A vulnerability has been identified in SICAM TOOLBOX II (All versions < V07.10). The affected application's database service is executed as `NT AUTHORITY\SYSTEM`.			
CVE-2023-38641	siemens - sicam toolbox ii	This could allow a local attacker to execute operating system commands with elevated privileges.	2023-08-08	7.8	High
	siemens - multiple	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process.			J
CVE-2023-38679	products	(ZDI-CAN-21106)	2023-08-08	7.8	High
	siemens - multiple	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process.			
CVE-2023-38680	products	(ZDI-CAN-21132)	2023-08-08	7.8	High
	siemens - multiple	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted IGS file. This could allow an attacker to execute code in the context of the current process.			
CVE-2023-38681	products siemens - multiple	(ZDI-CAN-21270)  A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted TIFF files. This could allow an attacker to execute code in	2023-08-08	7.8	High
CVE-2023-38682	products  siemens - multiple	the context of the current process.  A vulnerability has been identified in JT2Go (All versions < V14.2.0.5), Teamcenter Visualization V13.2 (All versions < V13.2.0.14), Teamcenter Visualization V14.1 (All versions < V14.1.0.10), Teamcenter Visualization V14.2 (All versions < V14.2.0.5). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted TIFF file. This could allow an attacker to execute code in	2023-08-08	7.8	High
CVE-2023-38683	products	the context of the current process.	2023-08-08	7.8	High
	siemens - multiple	A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to			
CVE-2023-39181	products	execute code in the context of the current process.	2023-08-08	7.8	High

		A vulnerability has been identified in Solid Edge SE2023 (All			
		versions < V223.0 Update 7). The affected applications contain an			
	siemens - multiple	out of bounds read past the end of an allocated structure while parsing specially crafted DFT files. This could allow an attacker to			
CVE-2023-39182	products	execute code in the context of the current process.	2023-08-08	7.8	High
<u> </u>	products	A vulnerability has been identified in Solid Edge SE2023 (All	2023 33 33	7.0	6
		versions < V223.0 Update 7). The affected applications contain an			
		out of bounds read past the end of an allocated structure while			
	siemens - multiple	parsing specially crafted PSM files. This could allow an attacker to			
CVE-2023-39183	products	execute code in the context of the current process.	2023-08-08	7.8	High
		A vulnerability has been identified in Solid Edge SE2023 (All versions < V223.0 Update 7). The affected applications contain an			
		out of bounds read past the end of an allocated structure while			
	siemens - multiple	parsing specially crafted PSM files. This could allow an attacker to			
CVE-2023-39184	products	execute code in the context of the current process.	2023-08-08	7.8	High
		A vulnerability has been identified in Solid Edge SE2023 (All			_
		versions < V223.0 Update 7). The affected applications contain an			
		out of bounds read past the end of an allocated structure while			
CVE 2022 2040E	siemens - multiple	parsing specially crafted PAR files. This could allow an attacker to	2022 00 00	7.0	11:
CVE-2023-39185	products	execute code in the context of the current process.  A vulnerability has been identified in Solid Edge SE2023 (All	2023-08-08	7.8	High
		versions < V223.0 Update 7). The affected applications contain an			
		out of bounds read past the end of an allocated structure while			
	siemens - multiple	parsing specially crafted DFT files. This could allow an attacker to			
VE-2023-39186	products	execute code in the context of the current process.	2023-08-08	7.8	High
		A vulnerability has been identified in Solid Edge SE2023 (All			
		versions < V223.0 Update 7). The affected applications contain an			
		out of bounds read past the end of an allocated structure while			
VE-2023-39187	siemens - multiple products	parsing specially crafted DFT files. This could allow an attacker to	2023-08-08	7.8	⊔iah
VE-2023-39167	products	execute code in the context of the current process.  A vulnerability has been identified in Solid Edge SE2023 (All	2023-06-06	7.0	High
		versions < V223.0 Update 7). The affected applications contain an			
		out of bounds read past the end of an allocated structure while			
	siemens - multiple	parsing specially crafted DFT files. This could allow an attacker to			
VE-2023-39188	products	execute code in the context of the current process.	2023-08-08	7.8	High
		A vulnerability has been identified in Solid Edge SE2023 (All			
		versions < V223.0 Update 7). The affected applications contain an			
	.•	out of bounds write past the end of an allocated structure while			
CVE-2023-39419	siemens -	parsing specially crafted DFT files. This could allow an attacker to	2023-08-08	7.8	⊔iah
.VE-2023-39419	solid_edge	execute code in the context of the current process.  A vulnerability has been identified in Solid Edge SE2023 (All	2023-08-08	7.8	High
		versions < V223.0 Update 2). The affected application contains a			
		use-after-free vulnerability that could be triggered while parsing			
		specially crafted DWG file. An attacker could leverage this			
	siemens -	vulnerability to execute code in the context of the current process.			
VE-2023-39549	solid_edge	(ZDI-CAN-19562)	2023-08-08	7.8	High
	microsoft - multiple				
:VE-2023-35359	products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
N/E 2022 25274	microsoft - multiple	Missassit Office Demosts Code Franchism Value and Hite	2022 00 00	7.0	11:-1-
VE-2023-35371	products microsoft - multiple	Microsoft Office Remote Code Execution Vulnerability	2023-08-08	7.8	High
CVE-2023-35372	products	Microsoft Office Visio Remote Code Execution Vulnerability	2023-08-08	7.8	High
VL-2023-33372	microsoft -	Wilciosoft Office visio Remote Code Execution vulnerability	2023-08-08	7.0	riigi
	windows_server_2	Reliability Analysis Metrics Calculation Engine (RACEng) Elevation			
VE-2023-35379	008	of Privilege Vulnerability	2023-08-08	7.8	High
	microsoft - multiple	,			
VE-2023-35380	products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
	microsoft - multiple				
VE-2023-35382	products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
	microsoft - multiple				
VE-2023-35386	products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
VE-2023-35390	microsoft - multiple products	.NET and Visual Studio Remote Code Execution Vulnerability	2023-08-08	7.8	High
VL-2023-33390	products	Untrusted search path in the installer for Zoom Desktop Client for	2023-08-08	7.0	riigi
		Windows before 5.14.5 may allow an authenticated user to enable			
VE-2023-36540	zoom - zoom	an escalation of privilege via local access.	2023-08-08	7.8	High
	microsoft - multiple				
VE-2023-36865	products	Microsoft Office Visio Remote Code Execution Vulnerability	2023-08-08	7.8	High
	microsoft - multiple				
VE-2023-36866	products	Microsoft Office Visio Remote Code Execution Vulnerability	2023-08-08	7.8	High
	microsoft - multiple			_	
VE-2023-36895	products	Microsoft Outlook Remote Code Execution Vulnerability	2023-08-08	7.8	High
VE 2022 26000	microsoft - multiple	Microsoft Eveal Romata Codo Evenution Vulnarability	2022 00 00	7.0	11:
VE-2023-36896	products microsoft - multiple	Microsoft Excel Remote Code Execution Vulnerability  Tablet Windows User Interface Application Core Remote Code	2023-08-08	7.8	High
VE-2023-36898	products	Execution Vulnerability	2023-08-08	7.8	High
, - L 2023 30030		Windows Common Log File System Driver Elevation of Privilege	2023 00 00	7.0	1 1151
	microsoft - multiple	I WILLIAUWS COLLILLIAITE EN VIELLI DI IVEL LIEVALIAITE ELIVIESE			

CVE-2023-36904	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2023-08-08	7.8	High
	microsoft - multiple				
CVE-2023-38154	products	Windows Kernel Elevation of Privilege Vulnerability	2023-08-08	7.8	High
	microsoft - hevc_video_extensi				
CVE-2023-38170	ons	HEVC Video Extensions Remote Code Execution Vulnerability	2023-08-08	7.8	High
<u> </u>	microsoft -	The state of the s		7.10	6
CVE-2023-38175	windows_defender	Microsoft Windows Defender Elevation of Privilege Vulnerability	2023-08-08	7.8	High
		Improper privilege management in Zoom Desktop Client for			
	zoom multiple	Windows and Zoom Rooms for Windows before 5.15.5 may allow			
CVE-2023-39211	zoom - multiple products	an authenticated user to enable an information disclosure via local access.	2023-08-08	7.8	High
	p. caucus	Adobe Dimension version 3.4.9 is affected by a Use After Free		7.10	6
		vulnerability that could result in arbitrary code execution in the			
		context of the current user. Exploitation of this issue requires user			
CVE-2023-38211	adobe - dimension	interaction in that a victim must open a malicious file.  Adobe Dimension version 3.4.9 is affected by a Heap-based Buffer	2023-08-09	7.8	High
		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			
CVE-2023-38212	adobe - dimension	file.	2023-08-09	7.8	High
CVE 2022 20670	samsung - multiple	Improper access control in HDCP trustlet prior to SMR Aug-2023	2022 00 40	7.0	
CVE-2023-30679	products samsung - multiple	Release 1 allows local attackers to execute arbitrary code.  Improper privilege management vulnerability in MMIGroup prior	2023-08-10	7.8	High
CVE-2023-30680	products	to SMR Aug-2023 Release 1 allows code execution with privilege.	2023-08-10	7.8	High
	p. 0 3 3 0 0	An improper input validation vulnerability within initialize function	1=3 00 10		0''
	samsung - multiple	in HAL VaultKeeper prior to SMR Aug-2023 Release 1 allows			
CVE-2023-30681	products	attacker to cause out-of-bounds write.	2023-08-10	7.8	High
CVE 2022 2000	samsung - multiple	Out-of-bounds Write in ReqDataRaw of libsec-ril prior to SMR Aug-	2022 00 40	7.0	111.1
CVE-2023-30686	products samsung - multiple	2023 Release 1 allows local attacker to execute arbitrary code.  Out-of-bounds Write in RmtUimApdu of libsec-ril prior to SMR	2023-08-10	7.8	High
CVE-2023-30687	products	Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
<u> </u>	products	Out-of-bounds Write in MakeUiccAuthForOem of libsec-ril prior to	2020 00 10	7.0	6
	samsung - multiple	SMR Aug-2023 Release 1 allows local attacker to execute arbitrary			
CVE-2023-30688	products	code.	2023-08-10	7.8	High
	10.1	Out-of-bounds Write in BuildOemEmbmsGetSigStrengthResponse			
CVE-2023-30689	samsung - multiple products	of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute arbitrary code.	2023-08-10	7.8	⊔iah
<u>CVE-2023-30069</u>	samsung - multiple	Parcel mismatch in AuthenticationConfig prior to SMR Aug-2023	2023-06-10	7.0	High
CVE-2023-30691	products	Release 1 allows local attacker to privilege escalation.	2023-08-10	7.8	High
	'	Out-of-bounds Write in			
		DoOemFactorySendFactoryBypassCommand of libsec-ril prior to			
01/5 0000 0000	samsung - multiple	SMR Aug-2023 Release 1 allows local attacker to execute arbitrary			
CVE-2023-30693	products	Code.	2023-08-10	7.8	High
	samsung - multiple	Out-of-bounds Write in IpcTxPcscTransmitApdu of libsec-ril prior to SMR Aug-2023 Release 1 allows local attacker to execute			
CVE-2023-30694	products	arbitrary code.	2023-08-10	7.8	High
	-	Out-of-bounds Write vulnerability in SSHDCPAPP TA prior to			
		"SAMSUNG ELECTONICS, CO, LTD System Hardware			
	samsung -	Update - 7/13/2023" in Windows Update for Galaxy book			
CVE-2023-30695	galaxy_book_go_fir	Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro 360 allows local attacker to execute arbitrary code.	2023-08-10	7.8	⊔iah
CVE-2023-30095	mware	An improper input validation in IpcTxGetVerifyAkey in libsec-ril	2023-06-10	7.0	High
	samsung - multiple	prior to SMR Aug-2023 Release 1 allows attacker to cause out-of-			
CVE-2023-30696	products	bounds write.	2023-08-10	7.8	High
		An improper input validation in IpcTxCfgSetSimlockPayload in			
O. (	samsung - multiple	libsec-ril prior to SMR Aug-2023 Release 1 allows attacker to cause			
CVE-2023-30697	products	out-of-bounds write.	2023-08-10	7.8	High
		Stack overflow vulnerability in SSHDCPAPP TA prior to "SAMSUNG ELECTONICS, CO, LTD System Hardware			
	samsung -	Update - 7/13/2023" in Windows Update for Galaxy book			
	galaxy_book_go_fir	Go, Galaxy book Go 5G, Galaxy book2 Go and Galaxy book2 Pro			
CVE-2023-30702	mware	360 allows local attacker to execute arbitrary code.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			_
		20.005.30467 (and earlier) are affected by an Violation of Secure			
		Design Principles vulnerability that could result in arbitrary code			
	adobe - multiple	execution in the context of the current user by bypassing the API blacklisting feature. Exploitation of this issue requires user			
CVE-2023-29320	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
	p. 5 3 4 5 5 5	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			0''
		20.005.30467 (and earlier) are affected by a Use After Free			
		vulnerability that could result in arbitrary code execution in the			
O. (	adobe - multiple	context of the current user. Exploitation of this issue requires user			
CVE-2023-38222	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
	adobe - multiple	20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer that could result in arbitrary code execution			

	T		T	ľ	
		requires user interaction in that a victim must open a malicious			
		file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by a Use After Free			
		vulnerability that could result in arbitrary code execution in the			
	adobe - multiple	context of the current user. Exploitation of this issue requires user			
CVE-2023-38224	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by a Use After Free			
		vulnerability that could result in arbitrary code execution in the			
0)/5 2022 20225	adobe - multiple	context of the current user. Exploitation of this issue requires user	2022 00 40	7.0	112.1
CVE-2023-38225	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of			
		Uninitialized Pointer vulnerability that could result in arbitrary			
		code execution in the context of the current user. Exploitation of			
	adobe - multiple	this issue requires user interaction in that a victim must open a			
CVE-2023-38226	products	malicious file.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by a Use After Free			
		vulnerability that could result in arbitrary code execution in the			
CVE 2022 20227	adobe - multiple	context of the current user. Exploitation of this issue requires user	2022 00 40	7.0	11:-1-
CVE-2023-38227	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use After Free			
		vulnerability that could result in arbitrary code execution in the			
	adobe - multiple	context of the current user. Exploitation of this issue requires user			
CVE-2023-38228	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
	·	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by an out-of-bounds write			
		vulnerability that could result in arbitrary code execution in the			
	adobe - multiple	context of the current user. Exploitation of this issue requires user			
CVE-2023-38231	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the			
	adobe - multiple	context of the current user. Exploitation of this issue requires user			
CVE-2023-38233	products	interaction in that a victim must open a malicious file.	2023-08-10	7.8	High
	p. 00.0.00	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and		7.10	6
		20.005.30467 (and earlier) are affected by an Access of			
		Uninitialized Pointer vulnerability that could result in arbitrary			
		code execution in the context of the current user. Exploitation of			
	adobe - multiple	this issue requires user interaction in that a victim must open a			
CVE-2023-38234	products	malicious file.	2023-08-10	7.8	High
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by an Access of			
		Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of			
	adobe - multiple	this issue requires user interaction in that a victim must open a			
CVE-2023-38246	products	malicious file.	2023-08-10	7.8	High
	p. 00.0.00	A use-after-free flaw was found in net/sched/cls_fw.c in classifiers		7.10	6
		(cls_fw, cls_u32, and cls_route) in the Linux Kernel. This flaw			
		allows a local attacker to perform a local privilege escalation due			
	linux - multiple	to incorrect handling of the existing filter, leading to a kernel			
CVE-2023-4128	products	information leak issue.	2023-08-10	7.8	High
	ivanti - multiple	Desktop & Server Management (DSM) may have a possible	2000 00 40		
CVE-2023-28129	products	execution of arbitrary commands.	2023-08-10	7.8	High
	intel -	Uncontrolled search path in some Intel(R) oneMKL software before version 2022.0 may allow an authenticated user to			
CVE-2022-25864	oneapi_math_kern el library	potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2022-23604	intel -	Improper access control in the Intel DTT Software before version	2023-00-11	7.0	півіі
	dynamic_tuning_te	8.7.10400.15482 may allow an authenticated user to potentially			
CVE-2022-29470	chnology	enable escalation of privilege via local access.	2023-08-11	7.8	High
	01	Improper input validation in some Intel(R) PROSet/Wireless WiFi			
	intel - multiple	and Killer(TM) WiFi software may allow an authenticated user to			
		potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
CVE-2022-38076	products	potentially chable escalation of privilege via local access.			
CVE-2022-38076	products	Uncontrolled search path in some Intel(R) RST software before		_	
CVE-2022-38076	·	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and		-	
	intel - multiple	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially			
	·	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
	intel - multiple	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.  Uncontrolled search path element in the Intel(R) Unite(R) Client			High
	intel - multiple	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.  Uncontrolled search path element in the Intel(R) Unite(R) Client software for Mac before version 4.2.11 may allow an			High
CVE-2022-43456	intel - multiple products	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.  Uncontrolled search path element in the Intel(R) Unite(R) Client software for Mac before version 4.2.11 may allow an authenticated user to potentially enable escalation of privilege via	2023-08-11	7.8	
CVE-2022-43456	intel - multiple	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.  Uncontrolled search path element in the Intel(R) Unite(R) Client software for Mac before version 4.2.11 may allow an authenticated user to potentially enable escalation of privilege via local access.			High High
CVE-2022-38076  CVE-2022-43456  CVE-2023-25182	intel - multiple products	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.  Uncontrolled search path element in the Intel(R) Unite(R) Client software for Mac before version 4.2.11 may allow an authenticated user to potentially enable escalation of privilege via local access.  Improper access control in the Intel(R) Unite(R) Hub software	2023-08-11	7.8	
CVE-2022-43456	intel - multiple products	Uncontrolled search path in some Intel(R) RST software before versions 16.8.5.1014.5, 17.11.3.1010.2, 18.7.6.1011.2 and 19.5.2.1049.5 may allow an authenticated user to potentially enable escalation of privilege via local access.  Uncontrolled search path element in the Intel(R) Unite(R) Client software for Mac before version 4.2.11 may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	

		Uncontrolled search path element in some Intel(R) VCUST Tool			
		software downloaded before February 3nd 2023 may allow an			
		authenticated user to potentially enable escalation of privilege via			
CVE-2023-25944	intel - vcust_tool	local access.	2023-08-11	7.8	High
	intel -	Improper input validation for the Intel(R) Easy Streaming Wizard			
CVE-2023-26587	easy_streaming_wi zard	software may allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
<u> </u>	2010	Incorrect default permissions in some Intel(R) Advanced Link	2023 00 11	7.0	111611
	intel -	Analyzer Standard Edition software installers before version 22.1			
	advanced_link_anal	.1 may allow an authenticated user to potentially enable			
CVE-2023-27505	yzer	escalation of privilege via local access.	2023-08-11	7.8	High
	intel -	Improper buffer restrictions in the Intel(R) Optimization for Tensorflow software before version 2.12 may allow an			
	optimization_for_t	authenticated user to potentially enable escalation of privilege via			
CVE-2023-27506	ensorflow	local access.	2023-08-11	7.8	High
	intel -	Improper access control in some Intel(R) ISPC software installers			
0) /5 2022 27502	ispc_software_inst	before version 1.19.0 may allow an authenticated user to	2022 00 44	7.0	
CVE-2023-27509	aller	potentially enable escalation of privileges via local access.  Uncontrolled search path in the Intel(R) Distribution of	2023-08-11	7.8	High
		OpenVINO(TM) Toolkit before version 2022.3.0 may allow an			
		authenticated user to potentially enable escalation of privilege via			
CVE-2023-28405	intel - openvino	local access.	2023-08-11	7.8	High
	intel -	Insecure inherited permissions in some Intel(R) oneMKL software			
CVE 2022 20650	oneapi_math_kern	before version 2022.0 may allow an authenticated user to	2022 00 11	70	Uiah
CVE-2023-28658	el_library intel -	potentially enable escalation of privilege via local access.  Incorrect default permissions in the Intel(R) ITS sofware before	2023-08-11	7.8	High
	intelligent_test_sys	version 3.1 may allow authenticated user to potentially enable			
CVE-2023-32543	tem	escalation of privilege via local access.	2023-08-11	7.8	High
		Improper buffer restrictions in some Intel(R) RealSense(TM) ID			
	intel -	software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may			
CVE-2023-32656	realsense_450_fa_f irmware	allow an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.8	High
<u>CVL 2023 32030</u>	intel -	Incorrect default permissions in some Intel(R) RealSense(TM) SDKs	2023 00 11	7.0	111611
	realsense_software	in version 0.25.0 may allow an authenticated user to potentially			
CVE-2023-32663	_development_kit	enable escalation of privilege via local access.	2023-08-11	7.8	High
		Improper buffer restrictions in some Intel(R) RealSense(TM) ID			
	intel - realsense_450_fa_f	software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an authenticated user to potentially enable escalation of			
CVE-2023-33867	irmware	privilege via local access.	2023-08-11	7.8	High
<u>CVL 2023 33007</u>	mmware	Out-of-bounds write in some Intel(R) RealSense(TM) ID software	2023 00 11	7.0	111611
	intel -	for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an			
	realsense_450_fa_f	authenticated user to potentially enable escalation of privilege via			
CVE-2023-33877	irmware	local access.	2023-08-11	7.8	High
	intel -	Protection mechanism failure in some Intel(R) RealSense(TM) ID software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may			
	realsense_450_fa_f	allow an authenticated user to potentially enable escalation of			
CVE-2023-34427	irmware	privilege via local access.	2023-08-11	7.8	High
	intel -	Race condition in some Intel(R) NUC BIOS firmware may allow a			
CVE 2022 24429	nuc_rugged_kit_nu	privileged user to potentially enable escalation of privilege via	2022 00 11	7.0	Hiab
CVE-2023-34438	c8cchb_firmware zohocorp -	local access.  The event analysis component in Zoho ManageEngine ADAudit	2023-08-11	7.8	High
	manageengine_ada	Plus 7.1.1 allows an attacker to bypass audit detection by creating			
CVE-2023-32783	udit_plus	or renaming user accounts with a "\$" symbol suffix.	2023-08-07	7.5	High
		B1i module of SAP Business One - version 10.0, application allows			
		an authenticated user with deep knowledge to send crafted			
		queries over the network to read or modify the SQL data. On successful exploitation, the attacker can cause high impact on			
CVE-2023-33993	sap - business_one	confidentiality, integrity and availability of the application.	2023-08-08	7.5	High
		Under certain conditions SAP Commerce (OCC API) - versions	1=3 23 33		
		HY_COM 2105, HY_COM 2205, COM_CLOUD 2211, endpoints			
		allow an attacker to access information which would otherwise be			
	can multiple	restricted. On successful exploitation there could be a high impact			
CVE-2023-37486	sap - multiple products	on confidentiality with no impact on integrity and availability of the application.	2023-08-08	7.5	High
<u> </u>	qualcomm -	Information disclosure in Network Services due to buffer over-read	2020 00-00	ر. ،	111811
CVE-2023-21625	apq8009_firmware	while the device receives DNS response.	2023-08-08	7.5	High
	qualcomm -	Transient DOS in Audio while remapping channel buffer in media			
CVE-2023-28555	ar8035_firmware	codec decoding.	2023-08-08	7.5	High
	siemens -	A vulnerability has been identified in RUGGEDCOM CROSSBOW (All versions < V5.4). The affected applications accept unauthenticated			
	ruggedcom_crossb	file write messages. An unauthenticated remote attacker could			
CVE-2023-37373	OW	write arbitrary files to the affected application's file system.	2023-08-08	7.5	High
		A vulnerability has been identified in RUGGEDCOM i800,			<del>_</del>
		RUGGEDCOM i800NC, RUGGEDCOM i801, RUGGEDCOM i801NC,			
		RUGGEDCOM i802, RUGGEDCOM i802NC, RUGGEDCOM i803,			
		RUGGEDCOM i803NC, RUGGEDCOM M2100, RUGGEDCOM			
		M2100E BLIGGEDCOM M2100NC BLIGGEDCOM M22200		l	
	siemens -	M2100F, RUGGEDCOM M2100NC, RUGGEDCOM M2200, RUGGEDCOM M2200F, RUGGEDCOM M2200NC, RUGGEDCOM			

	Т				
		RUGGEDCOM RMC30, RUGGEDCOM RMC30NC, RUGGEDCOM			
		RMC8388 V4.X, RUGGEDCOM RMC8388 V5.X, RUGGEDCOM RMC8388NC V4.X, RUGGEDCOM RMC8388NC V5.X, RUGGEDCOM			
		RP110, RUGGEDCOM RP110NC, RUGGEDCOM RS1600,			
		RUGGEDCOM RS1600F, RUGGEDCOM RS1600FNC, RUGGEDCOM			
		RS1600NC, RUGGEDCOM RS1600T, RUGGEDCOM RS1600TNC,			
		RUGGEDCOM RS400, RUGGEDCOM RS400F, RUGGEDCOM			
		RS400NC, RUGGEDCOM RS401, RUGGEDCOM RS401NC,			
		RUGGEDCOM RS416, RUGGEDCOM RS416F, RUGGEDCOM			
		RS416NC, RUGGEDCOM RS416NC v2, RUGGEDCOM RS416P,			
		RUGGEDCOM RS416PF, RUGGEDCOM RS416PNC, RUGGEDCOM			
		RS416PNC v2, RUGGEDCOM RS416Pv2, RUGGEDCOM RS416v2,			
		RUGGEDCOM RS8000, RUGGEDCOM RS8000A, RUGGEDCOM			
		RS8000ANC, RUGGEDCOM RS8000H, RUGGEDCOM RS8000HNC,			
		RUGGEDCOM RS8000NC, RUGGEDCOM RS8000T, RUGGEDCOM			
		RS8000TNC, RUGGEDCOM RS900, RUGGEDCOM RS900 (32M)			
		V4.X, RUGGEDCOM RS900 (32M) V5.X, RUGGEDCOM RS900F,			
		RUGGEDCOM RS900G, RUGGEDCOM RS900G (32M) V4.X,			
		RUGGEDCOM RS900G (32M) V5.X, RUGGEDCOM RS900GF, RUGGEDCOM RS900GNC, RUGGEDCOM RS900GNC(32M) V4.X,			
		RUGGEDCOM RS900GNC(32M) V5.X, RUGGEDCOM RS900GP,			
		RUGGEDCOM RS900GPF, RUGGEDCOM RS900GPNC, RUGGEDCOM			
		RS900L, RUGGEDCOM RS900LNC, RUGGEDCOM RS900M-GETS-			
		C01, RUGGEDCOM RS900M-GETS-XX, RUGGEDCOM RS900M-			
		STND-C01, RUGGEDCOM RS900M-STND-XX, RUGGEDCOM			
		RS900MNC-GETS-C01, RUGGEDCOM RS900MNC-GETS-XX,			
		RUGGEDCOM RS900MNC-STND-XX, RUGGEDCOM RS900MNC-			
		STND-XX-C01, RUGGEDCOM RS900NC, RUGGEDCOM			
		RS900NC(32M) V4.X, RUGGEDCOM RS900NC(32M) V5.X,			
		RUGGEDCOM RS900W, RUGGEDCOM RS910, RUGGEDCOM			
		RS910L, RUGGEDCOM RS910LNC, RUGGEDCOM RS910NC,			
		RUGGEDCOM RS910W, RUGGEDCOM RS920L, RUGGEDCOM			
		RS920LNC, RUGGEDCOM RS920W, RUGGEDCOM RS930L,			
		RUGGEDCOM RS930LNC, RUGGEDCOM RS930W, RUGGEDCOM			
		RS940G, RUGGEDCOM RS940GF, RUGGEDCOM RS940GNC,			
		RUGGEDCOM RS969, RUGGEDCOM RS969NC, RUGGEDCOM			
		RSG2100, RUGGEDCOM RSG2100 (32M) V4.X, RUGGEDCOM			
		RSG2100 (32M) V5.X, RUGGEDCOM RSG2100F, RUGGEDCOM			
		RSG2100NC, RUGGEDCOM RSG2100NC(32M) V4.X, RUGGEDCOM			
		RSG2100NC(32M) V5.X, RUGGEDCOM RSG2100P, RUGGEDCOM			
		RSG2100PF, RUGGEDCOM RSG2100PNC, RUGGEDCOM RSG2200,			
		RUGGEDCOM RSG2200F, RUGGEDCOM RSG2200NC, RUGGEDCOM RSG2288 V4.X, RUGGEDCOM RSG2288 V5.X, RUGGEDCOM			
		RSG2288NC V4.X, RUGGEDCOM RSG2288NC V5.X, RUGGEDCOM			
		RSG2300 V4.X, RUGGEDCOM RSG2300 V5.X, RUGGEDCOM			
		RSG2300F, RUGGEDCOM RSG2300NC V4.X, RUGGEDCOM			
		RSG2300NC V5.X, RUGGEDCOM RSG2300P V4.X, RUGGEDCOM			
		RSG2300P V5.X, RUGGEDCOM RSG2300PF, RUGGEDCOM			
		RSG2300PNC V4.X, RUGGEDCOM RSG2300PNC V5.X, RUGGEDCOM			
		RSG2488 V4.X, RUGGEDCOM RSG2488 V5.X, RUGGEDCOM			
		RSG2488F, RUGGEDCOM RSG2488NC V4.X, RUGGEDCOM			
		RSG2488NC V5.X, RUGGEDCOM RSG907R, RUGGEDCOM RSG908C,			
		RUGGEDCOM RSG909R, RUGGEDCOM RSG910C, RUGGEDCOM			
		RSG920P V4.X, RUGGEDCOM RSG920P V5.X, RUGGEDCOM			
		RSG920PNC V4.X, RUGGEDCOM RSG920PNC V5.X, RUGGEDCOM			
		RSL910, RUGGEDCOM RSL910NC, RUGGEDCOM RST2228,			
		RUGGEDCOM RST2228P, RUGGEDCOM RST916C, RUGGEDCOM			
		RST916P. The web server of the affected devices contains a			
		vulnerability that may lead to a denial of service condition.			
		An attacker may cause total loss of availability of the coals			
		An attacker may cause total loss of availability of the web server,			
	microsoft - multiple	which might recover after the attack is over.			
CVE-2023-35383	products	Microsoft Message Queuing Information Disclosure Vulnerability	2023-08-08	7.5	High
CVL-2023-33383	products	Buffer overflow in Zoom Clients before 5.14.5 may allow an	2023-00-0ŏ	7.3	ıııgıı
	zoom - multiple	unauthenticated user to enable a denial of service via network			
CVE-2023-36532	products	access.	2023-08-08	7.5	High
5.2 2023 30332	p. 50000	Uncontrolled resource consumption in Zoom SDKs before 5.14.7	_525 55 56	, .5	ייפייי
	zoom - multiple	may allow an unauthenticated user to enable a denial of service			
CVE-2023-36533	products	via network access.	2023-08-08	7.5	High
	microsoft - multiple	Windows Wireless Wide Area Network Service (WwanSvc)			<u> </u>
CVE-2023-36905	products	Information Disclosure Vulnerability	2023-08-08	7.5	High
	microsoft - multiple	Windows Cryptographic Services Information Disclosure			
CVE-2023-36906	products	Vulnerability	2023-08-08	7.5	High
	microsoft - multiple	Windows Cryptographic Services Information Disclosure			
CVE-2023-36907	products	Vulnerability	2023-08-08	7.5	High
	microsoft - multiple				
CVE-2023-36912	products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	7.5	High
01/5 0000 55515	microsoft - multiple		2020 25 55		
CVE-2023-36913	products	Microsoft Message Queuing Information Disclosure Vulnerability	2023-08-08	7.5	High

CVE-2023-38172	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	7.5	High
CVE-2023-38178	microsoft - multiple products	.NET Core and Visual Studio Denial of Service Vulnerability	2023-08-08	7.5	High
CVE-2023-38184	microsoft - multiple products	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	2023-08-08	7.5	High
	·	Improper input validation in Zoom SDK's before 5.14.10 may allow			
CVE 2022 20217	zoom - multiple products	an unauthenticated user to enable a denial of service via network	2023-08-08	7.5	⊔iah
CVE-2023-39217	microsoft - multiple	ASP.NET Core SignalR and Visual Studio Information Disclosure	2023-08-08	7.5	High
CVE-2023-35391	products	Vulnerability	2023-08-08	7.5	High
CVE-2023-38180	microsoft - multiple products	.NET and Visual Studio Denial of Service Vulnerability	2023-08-08	7.5	High
		Improper input validation vulnerability on the range header in			
CVE-2022-47185	apache - multiple products	Apache Software Foundation Apache Traffic Server. This issue affects Apache Traffic Server: through 9.2.1.	2023-08-09	7.5	High
		Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and			
		earlier) and 2.4.4-p4 (and earlier) are affected by a XML Injection (aka Blind XPath Injection) vulnerability that could lead in minor			
	adobe - multiple	arbitrary file system read. Exploitation of this issue does not			
CVE-2023-38207	products	require user interaction.	2023-08-09	7.5	High
		Cacti before 1.2.6 allows IDOR (Insecure Direct Object Reference)			
		for accessing any graph via a modified local_graph_id parameter to graph_xport.php. This is a different vulnerability than CVE-2019-			
CVE-2023-37543	cacti - cacti	16723.	2023-08-10	7.5	High
	0.00	A previously generated artifact by an administrator could be			
		accessed by an attacker. The contents of this artifact could lead to			
CVE-2023-32561	ivanti - avalanche	authentication bypass. Fixed in version 6.4.1.	2023-08-10	7.5	High
		Uncontrolled search path element in some Intel(R) Quartus(R) Prime Pro and Standard edition software for linux may allow an			
	intel - multiple	authenticated user to potentially enable escalation of privilege via			
CVE-2023-24016	products	local access.	2023-08-11	7.3	High
		Uncontrolled search path in some Intel(R) oneAPI Toolkit and			
	intal multiple	component software installers before version 4.3.1.493 may allow			
CVE-2023-28823	intel - multiple products	an authenticated user to potentially enable escalation of privilege via local access.	2023-08-11	7.3	High
<u> </u>	products	In DRM/oemcrypto, there is a possible out of bounds write due to	2023 00 11	7.5	111611
	google - multiple	an incorrect calculation of buffer size. This could lead to remote			
CVE-2023-33913	products	escalation of privilege with System execution privileges needed	2023-08-07	7.2	High
		In MongoDB Ops Manager v5.0 prior to 5.0.22 and v6.0 prior to			
	mongodb - multiple	6.0.17 it is possible for an authenticated user with project owner or project user admin access to generate an API key with the			
CVE-2023-4009	products	privileges of org owner resulting in privilege escalation.	2023-08-08	7.2	High
	microsoft -				
CVE-2023-38167	dynamics_365_busi ness_central	Microsoft Dynamics Business Central Elevation Of Privilege Vulnerability	2023-08-08	7.2	High
CVE-2023-36107	ness_central	Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and	2023-08-08	7.2	півіі
		earlier) and 2.4.4-p4 (and earlier) are affected by an Improper			
		Neutralization of Special Elements used in an OS Command ('OS			
	and a language of the state	Command Injection') vulnerability that could lead to arbitrary code			
CVE-2023-38208	adobe - multiple products	execution by an admin-privilege authenticated attacker.  Exploitation of this issue does not require user interaction.	2023-08-09	7.2	High
CVL 2023-30200	products	Exploration of this issue does not require user interaction.	2023-00-03	1.4	ıııgıı
		A vulnerability has been identified within Serv-U 15.4 that, if			
		exploited, allows an actor to bypass multi-factor/two-factor			
CVE-2023-35179	solarwinds - serv-u	authentication. The actor must have administrator-level access to	2022 00 11	7.2	Hiah
CVE-2023-35179	Solar Winus - Serv-u	Serv-U to perform this action.  Improper access control in some Intel(R) Unison(TM) software	2023-08-11	7.2	High
		before version 10.12 may allow a privileged user to potentially			
CVE-2023-25757	intel - unison	enable escalation of privilege via network access.	2023-08-11	7.2	High
CVE 2022 24525	qualcomm -	Cryptographic issue in HLOS due to improper authentication while	2022 02 02	7.4	
CVE-2023-21626	apq8009_firmware qualcomm -	performing key velocity checks using more than one key. Cryptographic issue in HLOS as derived keys used to	2023-08-08	7.1	High
	•	encrypt/decrypt information is present on stack after use.	2023-08-08	7.1	High
CVE-2023-21652	agt1000 firmware				
CVE-2023-21652	aqt1000_firmware microsoft -				
	microsoft - windows_server_2	Reliability Analysis Metrics Calculation (RacTask) Elevation of			
	microsoft -	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability	2023-08-08	7.1	High
	microsoft - windows_server_2	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability  The buffer obtained from kernel APIs such as	2023-08-08	7.1	High
	microsoft - windows_server_2	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability	2023-08-08	7.1	High
CVE-2023-21652 CVE-2023-36876	microsoft - windows_server_2	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability  The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g.	2023-08-08	7.1	High
CVE-2023-36876	microsoft - windows_server_2 008 qualcomm - fastconnect_6800_f	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability  The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-			
	microsoft - windows_server_2 008  qualcomm - fastconnect_6800_f irmware	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability  The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g.	2023-08-08	7.1	
CVE-2023-36876  CVE-2023-28576	microsoft - windows_server_2 008  qualcomm - fastconnect_6800_f irmware microsoft - multiple	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability  The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-bounds read/write issues.	2023-08-08	7	High
CVE-2023-36876	microsoft - windows_server_2 008  qualcomm - fastconnect_6800_f irmware	Reliability Analysis Metrics Calculation (RacTask) Elevation of Privilege Vulnerability  The buffer obtained from kernel APIs such as cam_mem_get_cpu_buf() may be readable/writable in userspace after kernel accesses it. In other words, user mode may race and modify the packet header (e.g. header.count), causing checks (e.g. size checks) in kernel code to be invalid. This may lead to out-of-			

missing bounds check. This could lead to local estatation of privilege with System execution privileges are aded. User interaction is not needed for exploitation. Patch 10: 2023-08-07 6,7 Medium for the products of the pro	I		In keyinstall, there is a possible out of bounds write due to a			
products products and products of the products						
CVE-2023-2028 products  ALPSO/282800 issue (D. ALPSO/282800).  In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for epiplotation. Pach ID: ALPSO/282800 issue (D. ALPSO/282800).  CVE-2023-20280 products  ALPSO/282800 issue (D. ALPSO/282800).  CVE-2023-20280 products  In rit, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges meded. User interaction is not needed for exploitation. Pach ID: ALPSO/282800 issue (D. ALPSO/282800).  CVE-2023-20295 products  ALPSO/282801 in rit, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not ended for exploitation. Pach ID: ALPSO/282800 issue (D. ALPSO/282800).  CVE-2023-20295 products  ALPSO/282801 in rit interes in a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not ended for exploitation. Pach ID: ALPSO/282800 issue (D. ALPSO/282800).  CVE-2023-20290 products  ALPSO/282801 issue (D. ALPSO/282801).  CVE-2023-20290 products  ALPSO/282801 issue (D. ALPSO/282801).  CVE-2023-20290 products  ALPSO/282801 issue (D. ALPSO/282801).  ALPSO/28280			privilege with System execution privileges needed. User			
In large install, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for expolation. Patch 10:  APS/07252895. Issue ID: APS/07256995.  CVF. 2023 20786 products  DVF. 2023 20786 products  In filtrer is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for expolation. Patch 10: AUSY/0785900. Issue ID: APS/07767811.  In filtrer is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for expolation. Patch ID: AUSY/07869000 issue ID: APS/0787891.  In carrier middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for expolation. Patch ID: AUSY/0788900 issue ID: APS/0787891.  In carrier middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for expolation. Patch ID: AUSY/0788912.  DVE 2023 20800 products products and products are interaction is not needed for expolation. Patch ID: AUSY/07889282.  DVE 2023 20807 products products and products produced for expolation privileges needed. User interaction is not needed for expolation. Patch ID: AUSY/0788938; use ID: AUSY/078893.  DVE 2023 20807 products products products and products produced for expolation privileges needed. User interaction is not needed for expolation. Patch ID: DVIVIS/058895, issue ID: AUSY/078893.  DVE 2023 20807 products	0.45		·			
missing bounds check. This could lead to local escalation of privilege with System execution privilege medical. Duer interaction is not needed for exploitation. Patch 10: APD/93289898; suse ID: APD/93289989; suse ID: APD/93289989; suse ID: APD/93289998; suse ID: APD/93289999; suse ID: APD/9328999; suse ID: APD/93289999; suse ID: APD/9328999; suse ID: APD/9328999; suse ID: APD/9328999; suse ID: APD/93289999; suse ID: APD/9328999; suse ID: APD/932	CVE-2023-20783	products		2023-08-07	6.7	Medium
products products provided products provided products provided products provided products provided products provided products pro						
App30782989; Essue ID: AP\$97829898. pascelled unt of pounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Liver is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges media. Part is a possible out of bounds write due to a missing bounds check						
ungs, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not received for exploitation. Part Int. 18, 1877,787811. But 18, 1877,787			interaction is not needed for exploitation. Patch ID:			
bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS0776911; Issue ID: 2023-08-07 6.7 Medium products In in it, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07864901. 2023-08-07 6.7 Medium In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: 2023-08-07 6.7 Medium Inc. 1997. Patch ID: 2023-08-07 6.7 Medium Inc. 2023-20800 products Inc. 2023-208	CVE-2023-20784	products		2023-08-07	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Park ID: JAMPS07767811, issue ID: ALPS07767811, issue ID: ALPS0776810, in rif, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privilege medical. User interaction is not needed for exploitation. Patch ID: ALPS07768901, issue ID: ALPS0776801, issue ID: ALPS0776901, issue ID						
poogle - multiple products  CVE-2023-20796  CVE-2023-20796  CVE-2023-20796  CVE-2023-20797  poogle - multiple products  CVE-2023-20797  products			•			
in in, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Park Dr. D. NEOPS/684900; Issue ID: ALPS/0764900; In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed or exploitation. Park ID: ALPS/0764905; Issue ID: ALPS/076490		google - multiple	, ,			
bounds check. This could lead to local escalation of privilege with System execution privilege needed. User interaction is not needed for exploitation. Patch ID: ALPS07864900; Issue ID: ALPS07866900.  CVE-2023-20792 products In camera middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS0782982; Issue ID: ALPS0782982. Patch ID: ALPS0782982; Issue ID: ALPS0782982. Patch ID: ALPS0782982; Issue ID: ALPS0782982; Is	CVE-2023-20786	products		2023-08-07	6.7	Medium
System execution privileges needed. User interaction is not not needed for exploitation. Patch ID. AIPS/7864090. Sissue ID: 2023-08-07 6.7 Medius for products and interaction is not needed for exploitation. Patch ID. AIPS/7864090. Sissue ID: 2023-08-07 6.7 Medius for privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: AIPS/7864093. Sissue ID: AIPS/7864093. Siss			•			
google - multiple products   ALPS07864909.   2023-08-07   6.7   Medius   CVE-2023-20795   2023-08-07   6.7   Medius   2023-08-07   6.7   Mediu			•			
CVE-2023-20895 products  ALES/07864900. 2023-08-07 6.7 Mediu  In camer a middleware, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALES/07839283. Issue ID: ALES/0783983. 2023-08-07 6.7 Mediu  CVE-2023-20806 products  No. 1 ng., there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALES/07806843; issue ID: ALES/0783437. 2023-08-07 6.7 Mediu  CVE-2023-20807 products  No. 1 ng., there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALES/07806843; issue ID: ALES/0780833 pounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DIV03645895; Issue ID: ALES/07808438 pounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DIV03654895; Issue ID: CVE-2023-20809 products  No. 1 n deep with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DIV03654895; Issue ID: CVE-2023-20811 products  No. 1 n deep with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DIV03654086; Issue ID: CVE-2023-20812 products  No. 2 not privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: CVE-2023-20813 products  No. 2 not privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: CVE-2023-20814 products  No. 2 not privilege with system execution priv		google - multiple				
to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID:  APS/072532825; Issue ID: ALPS/07259382;  In hop, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS/07357437.  In dipe, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS/07360843; Issue ID:  ALPS/07357437.  In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS/0760843; Issue ID:  ALPS/0736433.  In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID:  CVE-2023-20809 google - multiple products  In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV0365926; Issue ID:  CVE-2023-20810 google - multiple products  In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privilege exity security privilege with system execution privilege needed. User interaction is not needed for exploitation. Patch ID: DTV03659261; Issue ID:  CVE-2023-20810 products  In Wan service, there is a possible out of bounds write due to improper input validation is not needed for exploita	CVE-2023-20795		•	2023-08-07	6.7	Medium
google - multiple products			·			
google - multiple   products   APS07629582   susue ID AIPS07629582   susue ID AIPS07629682   susue I			<u> </u>			
Products   APS07629582   Issue ID: ALPS07629582   2023-08-07   6.7   Medium		google - multiple				
In hep, there is a possible out of bounds write due to a missing bounds. Scheck. This could lead to local escalation of privilege with system execution privileges. Needed. User interaction is not needed for exploitation. Patch ID: ALPS0734043; issue ID: ALPS07537437. In dipe, there is a possible out of bounds write due to a missing bounds. Scheck. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS074343; issue ID: ALPS0763443. In operation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS076343; issue ID: ALPS0763443. In operation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645395; issue ID: DTV03645895. In operation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV0364595; issue ID: DTV03645895. In operation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV0364595; issue ID: DTV03645895. In operation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV0375198; issue ID: DTV0375198. In IOMANUM, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV0361918; issue ID: DTV0364918; i	CVE-2023-20797		·	2023-08-07	6.7	Medium
bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07340433; Issue ID: 2023-08-07 6.7 Medium products  In dpc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS0768433; Issue ID: 2023-08-07 6.7 Medium In OPTEC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: 2023-08-07 6.7 Medium In OPTEC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03645895 is interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In OPTEC, Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In Value Patch ID: DTV03751198; Issue ID: 2023-08-07 6.7 Medium In Value Patch ID: DTV03751198; Issue ID: DTV03751198; Issue ID: DTV0375198; Issue ID:		p. 0 0 0 0 0		1_2 00 0,		
needed for exploitation. Patch ID: ALPS07340343; Issue ID: 2023-08-07 6.7 Medium			bounds check. This could lead to local escalation of privilege with			
APS07537437.  APS07537437.  In Oper Literal Expossible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: NPD07506433; Issue ID: APS07608433.  APS07608433.  In OPTE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: NPD07608435; Issue ID: DP0074654895.  OVE-2023-20808 google - android ID: DP003654895.  In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DP003751198; Issue ID: DP003751198.  OVE-2023-20809 products ID: DP003751198.  In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DP003751198; Issue ID: DP003751198.  In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DP0037510969041; Issue ID: DP00369061; ID:						
In ope, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO/060433, issue ID: ALPSO/160433, issue ID: DIVO3645895 issue ID: DIVO3645895 issue ID: DIVO3645895 issue ID: DIVO3645895; issue ID: DIVO3645895. In vide, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DIVO365198; issue ID: DIVO3751198; issue ID: DIVO3751198. In In MoMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DIVO3692061; issue ID: DIVO3692061 issue ID:	C/\E-3U33-3U6U8			ე <b>Ი</b> ᲔᲕ_Ი <b>ჹ</b> _Იჳ	6.7	Madium
bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608433; Issue ID: ALPS07608433.  In OPTE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03751198.  OVE-2023-20809 google - android In view of the products In Industry of the products Industry of the Industry of the	CVL-2U23-2U8U0	products		2023-06-07	0.7	ivieuluin
CVE-2023-20807 products ALPS07608433. In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges meted. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. In video, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895. In video, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198. In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061. Issue ID: DTV03692061. In Wan service, there is a possible out of bounds write due to improper inquive adiation. This could lead to local escalation of privilege with System execution privileges with System execution privileges meeded. User interaction is not needed for exploitation. Patch ID: DTV03692061. In Wan service, there is a possible out of bounds write due to improper inquive adiation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560. In Wan service, there is a possible out of bounds write due to improper inquive validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589. In wan service, there is a possible out of bounds write due to improper input validation. This could lea						
CVE-2023-20807 products   ALPS07608433.   2023-08-07   6.7   Mediu   In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges eneded. User interaction is not needed for exploitation. Patch ID: DYV03654895; Issue ID: 2023-08-07   6.7   Mediu   CVE-2023-20808   google - android   In Vede, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges eneded. User interaction is not needed for exploitation. Patch ID: DYV03751198; Issue ID: DYV03751198.   2023-08-07   6.7   Mediu   CVE-2023-20809   Mediu   CVE-2023-20809   Mediu   In Valor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DYV03652061; Issue ID: DYV03652061; Issue ID: DYV03692061.   2023-08-07   6.7   Mediu			System execution privileges needed. User interaction is not			
In OPTEE, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895, ISSUE ID: DTV03645895.  [OVE-2023-20809]  [OVE-2023-20810]  [OVE-2023-20810	OVE 2002 5555		·	2022 25 5-		
bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895.  [In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.  [In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.  [In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.  [In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.  [In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587; Issue ID: ALPS074535887.  [In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.  [In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	CVE-2023-20807	products		2023-08-07	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895.  In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03692061. In whan service, there is a possible out of bounds write due to Improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061. Issue ID: DTV03692061. In whan service, there is a possible out of bounds write due to Improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061. In what is not needed for exploitation. Patch ID: DTV03692061. In what is not needed for exploitation. Patch ID: DTV03692061. In what is not needed for exploitation of privileges with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061. In what needed for exploitation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061. In what needed for exploitation patch ID: DTV03692061. In what ne						
cyt-2023-20808   google - android   needed for exploitation. Patch ID: DTV03645895; Issue ID: DTV03645895.   2023-08-07   6.7   Medius   In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.   2023-08-07   6.7   Medius   DTV03752198   DTV03752198; Issue ID: DTV0375292061; ID: DTV03752061; ID: DTV0375292061; ID: DTV03						
In vdec, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.  In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.  CVE-2023-20811 products   In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061.  In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: APS07453560; Issue ID: APS07453560.  QUE-2023-20814 products   In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587; Issue ID: ALPS07453589.  QUE-2023-20815 products   In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.  QUE-2023-20816 products   In wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07435800; Issue ID: ALPS074535800.  A flaw was found in t			needed for exploitation. Patch ID: DTV03645895; Issue ID:			
bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.  In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.  In was service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587. Issue ID: ALPS07453588.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453580.  Question of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.  Question of privilege w	CVE-2023-20808	google - android		2023-08-07	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03751198; Issue ID: DTV03751198.  DTV03692061.  DTV03692061; Issue ID: DTV03692061; Issue ID: DTV03692061; Issue ID: DTV03692061.  In wina service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061.  ALPS07453560; Issue ID: ALPS07453560.  In wina service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587. Issue ID: ALPS07453587. Support of privileges with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587. Support of privileges with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.  DEVE-2023-20816  DEVE-2023-20816  DEVE-2023-20816  DEVE-2023-20817  DE			·			
CVE-2023-20819  google - multiple products  In wlan service, there is a possible out of bounds write due to improper input validation. Patch ID: ALPS07453587; Issue ID: ALPS07453589; Issue ID: ALPS07453589.  CVE-2023-20816  CVE-2023-20817  google - multiple products  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560.  CVE-2023-20815  CVE-2023-20815  CVE-2023-20815  CVE-2023-20816  ALPS07453587; Issue ID: ALPS07453587.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.  CVE-2023-20815  CVE-2023-20816  CVE-2023-20816  ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.  ALPS07453560; Issue ID: ALPS074535600.  ALPS07453600; Issue ID: ALPS07453600.  AFB07453600; Issue ID: ALPS07453600.  A			•			
In IOMMU, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges pneeded. User interaction is not needed for exploitation. Patch ID:  CVE-2023-20814		google - multiple	, ,			
bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.    In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.    In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:	CVE-2023-20809	products		2023-08-07	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061; Issue ID: DTV03692061.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453560; Issue ID: ALPS07453560.  2023-08-07 6.7 Medius products  ALPS07453560; Issue ID: ALPS07453560.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453587; Issue ID: ALPS07453587.  ALPS07453587; Issue ID: ALPS07453589.  ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  ALPS07453589; Issue ID: ALPS07453589.  ALPS07453580; Issue ID: ALPS07453589.  ALPS07453580; Issue ID: ALPS07453580.  ALPS07453600; Issue ID: ALPS07453600.  ALPS07453600; Issue ID: ALPS			·			
google - multiple products   DTV03692061.   Susue ID: DTV03692061; Issue ID: DTV03692061.   2023-08-07   6.7   Medium   In whan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.   2023-08-07   6.7   Medium   Medium			· ·			
DTV03692061.   DTV03692061.   2023-08-07   6.7   Medius   In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:		google - multiple	, ,			
improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453560; Issue ID: ALPS07453560.  2023-08-07 6.7 Medius interaction is not needed for exploitation. Patch ID:  ALPS07453580; Issue ID: ALPS07453587.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453587; Issue ID: ALPS07453587.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  ALPS07453589; Issue ID: ALPS07453600.  2023-08-07 6.7 Medius interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  2023-08-07 6.7 Medius interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  2023-08-07 6.7 Medius interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  2023-08-07 6.7 Medius interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  2023-08-07 6.7 Medius interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  2023-08-07 6.7 Medius interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  Aflaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name entries from a directory index and merging file name parts belonging to one file into a single long	CVE-2023-20811		·	2023-08-07	6.7	Medium
privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.  LIN wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.  LIN wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.  LIN wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.  LIN wan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged			·			
google - multiple products   Interaction is not needed for exploitation. Patch ID: ALPS07453560; Issue ID: ALPS07453560.   2023-08-07   6.7   Medium proper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.   2023-08-07   6.7   Medium proper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.   2023-08-07   6.7   Medium proper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.   2023-08-07   6.7   Medium proper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.   2023-08-07   6.7   Medium proper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.   2023-08-07   6.7   Medium proper input validation in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name entries from a directory index and merging file name parts belonging to one file into a single long file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged			· · · ·			
CVE-2023-20814 products ALPS07453560; Issue ID: ALPS07453560.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453587; Issue ID: ALPS07453587.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  CVE-2023-20816 products ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  CVE-2023-20817 products ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name entries from a directory index and merging file name parts belonging to one file into a single long file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged		google - multinle				
In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453587; Issue ID: ALPS07453587.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  2023-08-07 6.7 Medius In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privilege under the improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged	CVE-2023-20814		·	2023-08-07	6.7	Medium
privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453587; Issue ID: ALPS07453587.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: Begongle - multiple google - multiple products  ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name. Since the file name characters are copied into a stack variable, a local privileged			·			
google - multiple products    In war service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:						
ALPS07453587; Issue ID: ALPS07453587.    Discription of the products   Discription of the produc		googlol±l-	, , , , , , , , , , , , , , , , , , , ,			
In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name. Since the file name characters are copied into a stack variable, a local privileged	CVF-2023-20815		·	2023-08-07	6.7	Medium
improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged	OVE 2023-20013	products		2023 00-07	0.7	iviculuili
google - multiple products  ALPS07453589; Issue ID: ALPS07453589.  In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name. Since the file name characters are copied into a stack variable, a local privileged			·			
CVE-2023-20816 products ALPS07453589; Issue ID: ALPS07453589. 2023-08-07 6.7 Medium In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600. 2023-08-07 6.7 Medium A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name. Since the file name characters are copied into a stack variable, a local privileged			, , , , , , , , , , , , , , , , , , , ,			
In wlan service, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged	CVE 2022 20015		·	2022 22 27		N 4 - 11
improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:  ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged	CVE-2023-20816	products	·	2023-08-07	6.7	Medium
privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged						
google - multiple products interaction is not needed for exploitation. Patch ID: ALPS07453600; Issue ID: ALPS07453600.  A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged			· · · · ·			
A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file linux - multiple name characters are copied into a stack variable, a local privileged			interaction is not needed for exploitation. Patch ID:			
vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file linux - multiple name characters are copied into a stack variable, a local privileged	CVE-2023-20817	products	·	2023-08-07	6.7	Medium
reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged						
entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file linux - multiple name characters are copied into a stack variable, a local privileged			· · · · · · · · · · · · · · · · · · ·			
belonging to one file into a single long file name. Since the file linux - multiple name characters are copied into a stack variable, a local privileged						
linux - multiple name characters are copied into a stack variable, a local privileged			,			
CVE-2023-4273 products attacker could use this flaw to overflow the kernel stack. 2023-08-09 6.7 Medium			name characters are copied into a stack variable, a local privileged			
	CVE-2023-4273	products	attacker could use this flaw to overflow the kernel stack.	2023-08-09	6.7	Medium

CVE-2022-27635	intel - multiple products	Improper access control for some Intel(R) PROSet/Wireless WiFi and Killer(TM) WiFi software may allow a privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.7	Medium
	intel - nuc_8_compute_el ement_cm8i3cb4n_	Improper buffer restrictions in some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of			
CVE-2022-36372	firmware	privilege via local access.	2023-08-11	6.7	Medium
	intel - nuc_10_performan ce kit nuc10i7fnhn	Improper input validation in BIOS firmware for some Intel(R) NUC may allow a privileged user to potentially enable escalation of			
CVE-2022-37336	firmware	privilege via local access.	2023-08-11	6.7	Medium
<u> </u>	intel -	Improper access control in the BIOS firmware for some Intel(R)	2023 00 11	0.7	Wicaran
	atom_c3338r_firm	Processors may allow a privileged user to potentially enable			
CVE-2022-37343	ware	escalation of privilege via local access.	2023-08-11	6.7	Medium
		Improper access control for some Intel(R) PROSet/Wireless WiFi			
CVE 2022 40064	intel - multiple	and Killer(TM) WiFi software may allow a privileged user to	2022 00 11	6.7	Madius
CVE-2022-40964	products	potentially enable escalation of privilege via local access.  Unauthorized error injection in Intel(R) SGX or Intel(R) TDX for	2023-08-11	6.7	Mediun
	debian - multiple	some Intel(R) Xeon(R) Processors may allow a privileged user to			
CVE-2022-41804	products	potentially enable escalation of privilege via local access.	2023-08-11	6.7	Mediun
<u> </u>	p. 00.0.00	Protection mechanism failure for some Intel(R) PROSet/Wireless		0.7	
	intel - multiple	WiFi software may allow a privileged user to potentially enable			
CVE-2022-46329	products	escalation of privilege via local access.	2023-08-11	6.7	Mediun
	intel -				
	nuc_13_extreme_c				
	ompute_element_	Improper input validation in some Intel(R) NUC BIOS firmware may			
CVE 2022 22440	nuc13sbbi5_firmwa	allow a privileged user to potentially enable escalation of privilege	2022 00 44	6.7	N 4 = alia
CVE-2023-22449	re	via local access.	2023-08-11	6.7	Mediur
		Improper access control in some Intel(R) oneAPI Toolkit and component software installers before version 4.3.1.493 may allow			
	intel - multiple	a privileged user to potentially enable escalation of privilege via			
CVE-2023-27391	products	local access.	2023-08-11	6.7	Mediur
	intel -	Improper authorization in the Intel(R) NUC Pro Software Suite for		_	
	next_unit_of_comp	Windows before version 2.0.0.9 may allow a privileged user to			
CVE-2023-28385	uting_firmware	potentially enable escalation of privilage via local access.	2023-08-11	6.7	Mediur
	intel -				
	nuc_11_pro_kit_nu	Improper input validation in BIOS firmware for some Intel(R) NUCs			
0.45 2022 20404	c11tnhi70z_firmwa	may allow a privileged user to potentially enable escalation of	2022 20 44	6.7	
CVE-2023-29494	re	privilege via local access.	2023-08-11	6.7	Mediur
	intel -	Improper input validation in some Intel(R) NUC Rugged Kit, Intel(R) NUC Kit and Intel(R) Compute Element BIOS firmware may allow a			
	nuc_kit_nuc7i7bnh	privileged user to potentially enable escalation of privilege via			
CVE-2023-32617	x1_firmware	local access.	2023-08-11	6.7	Mediun
012 2020 02017	intel -	Improper input validation in some Intel(R) NUC BIOS firmware may	2023 00 11	0.7	Mediai
	nuc_rugged_kit_nu	allow a privileged user to potentially enable escalation of privilege			
CVE-2023-34086	c8cchb_firmware	via local access.	2023-08-11	6.7	Mediur
	microsoft -	Microsoft Edge (Chromium-based) Security Feature Bypass			
CVE-2023-38157	edge_chromium	Vulnerability	2023-08-07	6.5	Mediun
	netgear -	Netgear DGN3500 1.1.00.37 was discovered to contain a buffer			
CVE-2023-38924	dgn3500_firmware	overflow via the http_password parameter at setup.cgi.	2023-08-07	6.5	Mediun
		SAP NetWeaver Application Server ABAP and ABAP Platform -			
		versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752,			
		SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756,			
		SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804,			
		does not perform necessary authorization checks for an			
		authenticated user, resulting in escalation of privileges. This could			
	sap - multiple	allow an attacker to read sensitive information which can be used			
CVE-2023-37492	products	in a subsequent serious attack.	2023-08-08	6.5	Mediur
	qualcomm -	Information disclosure in Bluetooth when an GATT packet is			
CVE-2023-21647	qca6390_firmware	received due to improper input validation.	2023-08-08	6.5	Mediur
CVE 2022 25276	microsoft - multiple	Missesset Massaca Overving Denial of Coming Vulneyability	2022 00 00	C F	N/a divo
CVE-2023-35376	products microsoft - multiple	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Mediur
CVE-2023-35377	products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Mediur
<u>CVL 2023 33377</u>	microsoft - multiple	Wile 0501t Wessage Queuing Demai of Service Valiferability	2023 00 00	0.5	ivicalai
CVE-2023-35384	products	Windows HTML Platforms Security Feature Bypass Vulnerability	2023-08-08	6.5	Mediun
	microsoft - multiple	Microsoft Dynamics 365 On-Premises Remote Code Execution	<del>-</del>		1
CVE-2023-35389	products	Vulnerability	2023-08-08	6.5	Mediur
		Client-side enforcement of server-side security in Zoom clients			
	zoom - multiple	before 5.14.10 may allow an authenticated user to enable			
CVE-2023-36535	products	information disclosure via network access.	2023-08-08	6.5	Mediur
OUE 2255 5 5 5	microsoft - multiple		2000 5		
CVE-2023-36890	products	Microsoft SharePoint Server Information Disclosure Vulnerability	2023-08-08	6.5	Mediur
CVE 2022 2022	microsoft - multiple	Microsoft Outlook Specifing Vulnerahility	2022 00 00	6.5	N464!
CVE-2023-36893	products microsoft - multiple	Microsoft Outlook Spoofing Vulnerability	2023-08-08	6.5	Mediur

CVE-2023-36897	microsoft - multiple products	Visual Studio Tools for Office Runtime Spoofing Vulnerability	2023-08-08	6.5	Medium
CVE-2023-36908	microsoft - multiple products	Windows Hyper-V Information Disclosure Vulnerability	2023-08-08	6.5	Medium
CVE-2023-36909	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Medium
CVE-2023-38254	microsoft - multiple products	Microsoft Message Queuing Denial of Service Vulnerability	2023-08-08	6.5	Medium
		Improper input validation in Zoom Desktop Client for Windows			
CVE 2022 20200		before 5.15.5 may allow an authenticated user to enable an	2022 00 00	6.5	NA a altituda
CVE-2023-39209	zoom - zoom	information disclosure via network access.  Adobe Commerce versions 2.4.6-p1 (and earlier), 2.4.5-p3 (and	2023-08-08	6.5	Medium
		earlier) and 2.4.4-p4 (and earlier) are affected by an Incorrect Authorization vulnerability that could lead to a Security feature			
		bypass. A low-privileged attacker could leverage this vulnerability			
CVE-2023-38209	adobe - multiple products	to access other user's data. Exploitation of this issue does not require user interaction.	2023-08-09	6.5	Medium
	intel - multiple	Improper input validation in some Intel(R) PROSet/Wireless WiFi			
CVE-2022-36351	products	and Killer(TM) WiFi software may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2023-08-11	6.5	Medium
		Information exposure through microarchitectural state after transient execution in certain vector execution units for some			
	redhat - multiple	Intel(R) Processors may allow an authenticated user to potentially			
CVE-2022-40982	products	enable information disclosure via local access.  In audio, there is a possible out of bounds write due to a missing	2023-08-11	6.5	Medium
		bounds check. This could lead to local escalation of privilege with			
	google - multiple	System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628524; Issue ID:			
CVE-2023-20785	products	ALPS07628524.  In thermal, there is a possible use after free due to a race	2023-08-07	6.4	Medium
		condition. This could lead to local escalation of privilege with			
		System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID:			
CVE-2023-20787	google - android	ALPS07648734.	2023-08-07	6.4	Medium
		In thermal, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with			
		System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648734; Issue ID:			
CVE-2023-20788	google - android	ALPS07648735.	2023-08-07	6.4	Medium
	intel - nuc_performance_				
	kit_and_mini_pc_n	Race condition in some Intel(R) NUC BIOS firmware may allow a			
CVE-2023-34349	uc10i3fnh_firmwar e	privileged user to potentially enable escalation of privilege via local access.	2023-08-11	6.4	Medium
CVE-2023-36869	microsoft - multiple products	Azure DevOps Server Spoofing Vulnerability	2023-08-08	6.3	Medium
<u>CVL-2023-30803</u>	products	In SAP NetWeaver Process Integration - versions SAP_XIESR 7.50,	2023-08-08	0.3	Mediaiii
	sap -	SAP_XITOOL 7.50, SAP_XIAF 7.50, user-controlled inputs, if not sufficiently encoded, could result in Cross-Site Scripting (XSS)			
CVE 2022 27400	netweaver_process	attack. On successful exploitation the attacker can cause limited	2022 00 00	C 4	na di sa
CVE-2023-37488	_integration zohocorp - multiple	impact on confidentiality and integrity of the system.  Zoho ManageEngine Applications Manager through 16530 allows	2023-08-08	6.1	Medium
CVE-2023-38333	products zohocorp -	reflected XSS while logged in. Cross Site Scripting (XSS) vulnerability in Query Report feature in	2023-08-10	6.1	Medium
	manageengine_pas	Zoho ManageEngine Password Manager Pro version 11001, allows			
CVE-2020-27449	sword_manager_pr o	remote attackers to execute arbitrary code and steal cookies via crafted JavaScript payload.	2023-08-11	6.1	Medium
	microsoft -				
CVE-2023-36873	.net_framework	.NET Framework Spoofing Vulnerability SAP Supplier Relationship Management -versions 600, 602, 603,	2023-08-08	5.9	Medium
		604, 605, 606, 616, 617, allows an unauthorized attacker to discover information relating to SRM within Vendor Master Data			
		for Business Partners replication functionality. This information			
CVE-2023-39436	sap - multiple products	could be used to allow the attacker to specialize their attacks against SRM.	2023-08-08	5.8	Medium
		In Contacts Service, there is a possible missing permission			2 2 3 1
CVE-2023-33906	google - multiple products	check. This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
	google - multiple	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional			
CVE-2023-33907	products	execution privileges	2023-08-07	5.5	Medium
	google - multiple	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional			
CVE-2023-33908	products	execution privileges	2023-08-07	5.5	Medium
	google - multiple	In Contacts service, there is a possible missing permission check. This could lead to local information disclosure with no			
CVE-2023-33909	products	additional execution privileges	2023-08-07	5.5	Medium

CVE-2023-33910	google - multiple products	In Contacts Service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-08-07	5.5	Medium
		In vowifi service, there is a possible missing permission check. This			
	google - multiple	could lead to local information disclosure with no additional			
CVE-2023-33911	products	execution privileges	2023-08-07	5.5	Mediun
		In Contacts service, there is a possible missing permission			
	google - multiple	check.This could lead to local information disclosure with no			
CVE-2023-33912	products	additional execution privileges	2023-08-07	5.5	Mediun
	P	A flaw was found in the Linux kernel's TUN/TAP functionality. This			
		issue could allow a local user to bypass network filters and gain			
		,,			
		unauthorized access to some resources. The original patches fixing			
		CVE-2023-1076 are incorrect or incomplete. The problem is that			
		the following upstream commits - a096ccca6e50 ("tun:			
		tun_chr_open(): correctly initialize socket uid"), - 66b2c338adce			
		("tap: tap_open(): correctly initialize socket uid"), pass "inode-			
	linux - multiple	>i_uid" to sock_init_data_uid() as the last parameter and that			
CVE-2023-4194	products	turns out to not be accurate.	2023-08-07	5.5	Mediur
		A vulnerability has been identified in Parasolid V34.1 (All versions			
		< V34.1.258), Parasolid V35.0 (All versions < V35.0.254), Parasolid			
		V35.1 (All versions < V35.1.171), Teamcenter Visualization V14.1			
		(All versions), Teamcenter Visualization V14.2 (All versions <			
		V14.2.0.6), Teamcenter Visualization V14.3 (All versions). The		1	
		affected application contains a stack exhaustion vulnerability while		1	
	siemens - multiple	parsing a specially crafted X_T file. This could allow an attacker to		1	
CVE-2023-38532	products	cause denial of service condition.	2023-08-08	5.5	Mediur
	microsoft - multiple				
CVE-2023-36889	products	Windows Group Policy Security Feature Bypass Vulnerability	2023-08-08	5.5	Mediur
	microsoft - multiple	Windows Smart Card Resource Management Server Security			carar
CVE_2022 2604.4		,	2022 00 00	E F	Madium
CVE-2023-36914	products	Feature Bypass Vulnerability	2023-08-08	5.5	Mediur
	zoom -	Cleartext storage of sensitive information in Zoom Client SDK for			
	meeting_software_	Windows before 5.15.0 may allow an authenticated user to enable			
CVE-2023-39210	development_kit	an information disclosure via local access.	2023-08-08	5.5	Mediur
		Untrusted search path in Zoom Rooms for Windows before version			
		5.15.5 may allow an authenticated user to enable a denial of			
CVE 2022 20212	Zoom rooms	service via local access.	2023-08-08	5.5	Mediur
CVE-2023-39212	zoom - rooms		2023-08-08	5.5	iviediui
		Adobe Dimension version 3.4.9 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			
CVE-2023-38213	adobe - dimension	interaction in that a victim must open a malicious file.	2023-08-09	5.5	Mediun
012 2020 00210	adobe differential	Improper access control vulnerability in SLocationService prior to	2020 00 03		Wiedian
	comerung multiple	SMR Aug-2023 Release 1 allows local attacker to update fake			
CVE 2022 20CE4	samsung - multiple	·	2022 00 40		N 4 = =1:
CVE-2023-30654	products	location.	2023-08-10	5.5	Mediun
		Improper access control vulnerability in TelephonyUI prior to SMR			
	samsung - multiple	Aug-2023 Release 1 allows local attacker to connect BLE without			
CVE-2023-30698	products	privilege.	2023-08-10	5.5	Mediur
	samsung - multiple	PendingIntent hijacking in WifiGeofenceManager prior to SMR			
CVE-2023-30701	products	Aug-2023 Release 1 allows local attacker to arbitrary file access.	2023-08-10	5.5	Mediun
	p. comment	Improper sanitization of incoming intent in Galaxy Store prior to			
	comcuna	version 4.5.56.6? allows local attackers to access privileged content			
CVE 2022 2070E	samsung -		2022 00 10		Madium
CVE-2023-30705	galaxy_store	providers as Galaxy Store permission.	2023-08-10	5.5	Mediur
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and		İ	
		20.005.30467 (and earlier) are affected by a Use After Free		ĺ	
		vulnerability that could lead to disclosure of sensitive memory. An		ĺ	
		attacker could leverage this vulnerability to bypass mitigations		ĺ	
		, ,,		İ	
	adobe - multiple	I SUCH AS ASEK. EXDIDITATION OF THIS ISSUE PENTITES HISE INTERACTION IN			l
CVE-2023-20303	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in	2023 <u>-</u> 08-10	55	
CVE-2023-29303	adobe - multiple products	that a victim must open a malicious file.	2023-08-10	5.5	Mediur
CVE-2023-29303	· ·	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled	2023-08-10	5.5	Mediur
CVE-2023-29303	products	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker	2023-08-10	5.5	Mediur
CVE-2023-29303	products adobe -	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-	2023-08-10	5.5	Mediur
CVE-2023-29303	products	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker	2023-08-10	5.5	Mediur
CVE-2023-29303	products adobe -	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-	2023-08-10	5.5	Mediur
	adobe - xmp_toolkit_softw are_development_	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a			
	products  adobe - xmp_toolkit_softw	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-08-10	5.5	
	adobe - xmp_toolkit_softw are_development_	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
	adobe - xmp_toolkit_softw are_development_	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read			
	adobe - xmp_toolkit_softw are_development_	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An			
	adobe - xmp_toolkit_softw are_development_	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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			
	adobe - xmp_toolkit_softw are_development_	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An			
CVE-2023-38210	adobe - xmp_toolkit_softw are_development_ kit	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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			Mediur
CVE-2023-38210	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (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.	2023-08-10	5.5	Mediur
CVE-2023-38210	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	2023-08-10	5.5	Mediur
CVE-2023-38210	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free	2023-08-10	5.5	Mediur
CVE-2023-38210	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An	2023-08-10	5.5	Mediur
CVE-2023-38210	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	2023-08-10	5.5	Mediur
CVE-2023-38210	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An	2023-08-10	5.5	Mediur
CVE-2023-38210  CVE-2023-38229  CVE-2023-38230	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple products	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by a Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	2023-08-10	5.5	Mediur
CVE-2023-38210 CVE-2023-38229	adobe - xmp_toolkit_softw are_development_ kit  adobe - multiple products  adobe - multiple	that a victim must open a malicious file.  Adobe XMP Toolkit versions 2022.06 is affected by a Uncontrolled Resource Consumption vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are 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	2023-08-10	5.5	Mediun Mediun Mediun

		vulnerability that could lead to disclosure of sensitive memory. An			
		attacker could leverage this vulnerability to bypass mitigations			
		such as ASLR. Exploitation of this issue requires user interaction in			
		that a victim must open a malicious file.			
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38235	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
011 1013 00103	products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	2023 00 20	3.3	· · · · · · · · · · · · · · · · · · ·
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38236	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38237	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
	p. comoco	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by a Use-After-Free			
		vulnerability that could lead to disclosure of sensitive memory. An			
		attacker could leverage this vulnerability to bypass mitigations			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38238	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by an out-of-bounds read			
		vulnerability that could lead to disclosure of sensitive memory. An			
	ماملان می امام	attacker could leverage this vulnerability to bypass mitigations			
CVE 2022 20220	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in	2023-08-10	5.5	Madius
CVE-2023-38239	products	that a victim must open a malicious file.  Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	2023-08-10	5.5	Mediun
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38240	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
	'	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38241	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38242	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
<u> </u>	products	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	2023 00 10	3.3	Wicaran
		20.005.30467 (and earlier) are affected by a Use-After-Free			
		vulnerability that could lead to disclosure of sensitive memory. An			
		attacker could leverage this vulnerability to bypass mitigations			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38243	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediur
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38244	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediur
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could			
		leverage this vulnerability to obtain NTLMv2 credentials.			
		Exploitation of this issue requires user interaction in that a victim			
	adobe - multiple	must open a maliciously crafted Microsoft Office file, or visit an			
CVE-2023-38245	products	attacker controlled web page.	2023-08-10	5.5	Mediun
	p. 00.000	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and	2_2 00 10		
		20.005.30467 (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			
	adobe - multiple	such as ASLR. Exploitation of this issue requires user interaction in			
CVE-2023-38247	products	that a victim must open a malicious file.	2023-08-10	5.5	Mediun
	adobe - multiple	Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
CVE-2023-38248	products	20.005.30467 (and earlier) are affected by an out-of-bounds read	2023-08-10	5.5	Medium

		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.			
		Use of hard-coded credentials in some Intel(R) Unison(TM)			
CV		software before version 10.12 may allow an authenticated user	2022 00 44		
CVE-2022-44612	intel - unison	user to potentially enable information disclosure via local access.	2023-08-11	5.5	Mediur
	intel - onevpl_gpu_runtim	Out-of-bounds read in some Intel(R) oneVPL GPU software before version 22.6.5 may allow an authenticated user to potentially			
CVE-2023-22338	e e	enable information disclosure via local access.	2023-08-11	5.5	Mediur
CVL 2023 22330	intel -	Improper neutralization in software for the Intel(R) oneVPL GPU	2023 00 11	3.3	ivicalai
	onevpl_gpu_runtim	software before version 22.6.5 may allow an authenticated user to			
CVE-2023-22840	e	potentially enable denial of service via local access.	2023-08-11	5.5	Mediur
		Insufficient control flow management in the Hyperscan Library			
		maintained by Intel(R) before version 5.4.1 may allow an			
	intel -	authenticated user to potentially enable denial of service via local			
CVE-2023-28711	hyperscan_library	access.	2023-08-11	5.5	Mediur
	2.1.1	Out-of-bounds read in some Intel(R) RealSense(TM) ID software			
	intel -	for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may allow an			
CVE-2023-30760	realsense_450_fa_f irmware	authenticated user to potentially enable information disclosure via local access.	2023-08-11	5.5	Mediur
CVE-2023-30760	IIIIware	Improper access control in the Intel Unite(R) android application	2023-06-11	3.3	Mediui
		before version 4.2.3504 may allow an authenticated user to			
CVE-2023-32609	intel - unite	potentially enable information disclosure via local access.	2023-08-11	5.5	Mediun
<u> </u>	micer diffic	Insufficient input validation and sanitation in Weblog Category	2023 00 11	3.3	Wicaran
		name, Website About and File Upload features in all versions of			
		Apache Roller on all platforms allows an authenticated user to			
		perform an XSS attack. Mitigation: if you do not have Roller			
		configured for untrusted users, then you need to do nothing			
		because you trust your users to author raw HTML and other web			
		content. If you are running with untrusted users then you should			
0.45 0000 0000		upgrade to Roller 6.1.2 and you should disable Roller's File Upload			
CVE-2023-37581	apache - roller	feature.?	2023-08-06	5.4	Mediur
		SAP business One allows - version 10.0, allows an attacker to insert malicious code into the content of a web page or application and			
		gets it delivered to the client, resulting to Cross-site scripting. This			
		could lead to harmful action affecting the Confidentiality, Integrity			
CVE-2023-39437	sap - business_one	and Availability of the application.	2023-08-08	5.4	Mediun
CVL 2023 33437	Sup Business_one	Due to missing authentication check in SAP Host Agent - version	2023 00 00	J. <del>1</del>	Wicaran
		7.22, an unauthenticated attacker can set an undocumented			
		parameter to a particular compatibility value and in turn call read			
		functions. This allows the attacker to gather some non-sensitive			
		information about the server. There is no impact on integrity or			
CVE-2023-36926	sap - host_agent	availability.	2023-08-08	5.3	Mediun
		SAP PowerDesigner - version 16.7, queries all password hashes in			
		the backend database and compares it with the user provided one			
CVE 2022 27404	sap -	during login attempt, which might allow an attacker to access	2022 00 00	г э	N 4 o di cue
CVE-2023-37484	powerdesigner	password hashes from the client's memory.	2023-08-08	5.3	Mediun
		SAP Business One (Service Layer) - version 10.0, allows an authenticated attacker with deep knowledge perform certain			
		operation to access unintended data over the network which			
		could lead to high impact on confidentiality with no impact on			
CVE-2023-37487	sap - business_one	integrity and availability of the application	2023-08-08	5.3	Mediun
	<u> </u>	, , , ,			
		A CWE-119: Improper Restriction of Operations within the Bounds			
		of a Memory			
		Buffer vulnerability exists that could cause memory corruption			
	schneider-electric -	when an authenticated user			
CVE-2023-3953	pro-face_gp-pro_ex	opens a tampered log file from GP-Pro EX.	2023-08-09	5.3	Mediur
		Client-side enforcement of server-side security in Zoom clients			
0) /5 2022 2024 0	zoom - multiple	before 5.14.10 may allow a privileged user to enable information	2022 00 00	4.0	
CVE-2023-39218	products	disclosure via network access.	2023-08-08	4.9	Mediur
		Adobe Acrobat Reader versions 23.003.20244 (and earlier) and			
		20.005.30467 (and earlier) are affected by an Untrusted Search			
		Path vulnerability that could lead to Application denial-of-service.  An attacker could leverage this vulnerability if the default			
		PowerShell Set-ExecutionPolicy is set to Unrestricted, making the			
	adobe - multiple	attack complexity high. Exploitation of this issue requires user			
CVE-2023-29299	products	interaction in that a victim must open a malicious file.	2023-08-10	4.7	Mediur
	microsoft -	·			
CVE-2023-35394	azure_hdinsights	Azure HDInsight Jupyter Notebook Spoofing Vulnerability	2023-08-08	4.6	Mediun
		Improper Authorization vulnerability in Samsung Internet prior to			
		version 22.0.0.35 allows physical attacker access downloaded files			
	i .	in Secret Mode without user authentication.	2023-08-10	4.6	Mediun
CVE-2023-30704	samsung - internet		2020 00 10		
CVE-2023-30704	samsung - internet		2023 00 10		
CVE-2023-30704	samsung - internet		2020 00 10		
CVE-2023-30704	samsung - internet		2023 33 13		

CVE-2023-35393	microsoft - azure_hdinsights	Azure Apache Hive Spoofing Vulnerability	2023-08-08	4.5	Medium
CVE-2023-36877	microsoft -	Azure Apache Oozie Spoofing Vulnerability	2023-08-08	4.5	Medium
CVE-2023-30677	azure_hdinsights microsoft -	Azdre Apache Gozie Spooting Vullerability	2023-06-06	4.5	Medium
CVE-2023-36881	azure_hdinsights microsoft -	Azure Apache Ambari Spoofing Vulnerability	2023-08-08	4.5	Medium
CVE-2023-38188	azure_hdinsights	Azure Apache Hadoop Spoofing Vulnerability	2023-08-08	4.5	Medium
	google - multiple	In camera driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service			
CVE-2022-47350	products	with System execution privileges needed	2023-08-07	4.4	Medium
	google - multiple	In camera driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service			
CVE-2022-47351	products	with System execution privileges needed  In keyinstall, there is a possible information disclosure due to a	2023-08-07	4.4	Medium
		missing bounds check. This could lead to local information			
	google - multiple	disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:			
CVE-2023-20780	products	ALPS08017756; Issue ID: ALPS08017756.	2023-08-07	4.4	Medium
		In keyinstall, there is a possible memory corruption due to a missing bounds check. This could lead to local denial of service			
	google - multiple	with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08017756; Issue ID:			
CVE-2023-20781	products	ALPS07905323.	2023-08-07	4.4	Medium
		In keyinstall, there is a possible information disclosure due to a missing bounds check. This could lead to local information			
		disclosure with System execution privileges needed. User			
CVE-2023-20782	google - multiple products	interaction is not needed for exploitation. Patch ID: ALPS07550104; Issue ID: ALPS07550103.	2023-08-07	4.4	Medium
		In jpeg, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with			
		System execution privileges needed. User interaction is not			
CVE-2023-20789	google - multiple products	needed for exploitation. Patch ID: ALPS07693193; Issue ID: ALPS07693193.	2023-08-07	4.4	Medium
<u>CVL 2023 20703</u>	products	In apu, there is a possible memory corruption due to a missing	2023 00 07	7.7	IVICUIUII
		bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is not			
CVE 2022 20702	google - multiple	needed for exploitation. Patch ID: ALPS07767818; Issue ID:	2022 00 07	4.4	
CVE-2023-20793	products	ALPS07767818.  In pda, there is a possible out of bounds read due to an incorrect	2023-08-07	4.4	Medium
		calculation of buffer size. This could lead to local information disclosure with System execution privileges needed. User			
	google - multiple	interaction is not needed for exploitation. Patch ID:			
CVE-2023-20798	products	ALPS07147572; Issue ID: ALPS07421076.  In IOMMU, there is a possible information disclosure due to	2023-08-07	4.4	Medium
		improper input validation. This could lead to local information			
	google - multiple	disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03692061;			
CVE-2023-20810	products	Issue ID: DTV03692061.  In wlan service, there is a possible out of bounds read due to	2023-08-07	4.4	Medium
		improper input validation. This could lead to local information			
	google - multiple	disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:			
CVE-2023-20813	products	ALPS07453549; Issue ID: ALPS07453549.	2023-08-07	4.4	Medium
		In wlan service, there is a possible out of bounds read due to improper input validation. This could lead to local information			
	google - multiple	disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:			
CVE-2023-20818	products	ALPS07460540; Issue ID: ALPS07460540.	2023-08-07	4.4	Medium
		In SAP BusinessObjects Business Intelligence - version 420, If a user logs in to a particular program, under certain specific			
		conditions memory might not be cleared up properly, due to			
	sap - businessobjects_bu	which attacker might be able to get access to user credentials. For a successful attack, the attacker needs to have local access to the			
CVE-2023-39440	siness_intelligence	system. There is no impact on availability and integrity.	2023-08-08	4.4	Medium
	intel - pentium_j6426_fir	Improper buffer restrictions in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable			
CVE-2022-27879	mware	information disclosure via local access.  Improper input validation in firmware for some Intel(R) PCSD BIOS	2023-08-11	4.4	Medium
		before version 02.01.0013 may allow a privileged user to			
CVE-2022-34657	intel - pcsd_bios	potentially enable information disclosure via local access.  Improper initialization in the BIOS firmware for some Intel(R)	2023-08-11	4.4	Medium
CVE 2022 2003	intel - xeon_d-	Processors may allow a privileged user to potentially enable	2022 00 41		N.A !!
CVE-2022-38083	2745nx_firmware intel -	information disclosure via local access.  Improper Input validation in firmware for some Intel(R) Converged	2023-08-11	4.4	Medium
	converged_security _management_eng	Security and Management Engine before versions 15.0.45, and 16.1.27 may allow a privileged user to potentially enable denial of			
CVE-2022-38102	ine_firmware	service via local access.	2023-08-11	4.4	Medium

					1
	intel -	Insufficient control flow management in the BIOS firmware for			
	pentium_j6426_fir	some Intel(R) Processors may allow a privileged user to potentially			
CVE-2022-43505	mware	enable denial of service via local access.	2023-08-11	4.4	Medium
	intel -				
	nuc_11_performan	Use of uninitialized resource in some Intel(R) NUC BIOS firmware			
	ce_kit_nuc11pahi3	may allow a privileged user to potentially enable information			
CVE-2023-22330	_firmware	disclosure via local access.	2023-08-11	4.4	Medium
	intel -				
	nuc_7_enthusiast_	Improper initialization in some Intel(R) NUC BIOS firmware may			
	nuc7i7bnkq_firmw	allow a privileged user to potentially enable information disclosure			
CVE-2023-22356	are	via local access.	2023-08-11	4.4	Medium
		Improper initialization in some Intel(R) NUC 13 Extreme Compute			
		Element, Intel(R) NUC 13 Extreme Kit, Intel(R) NUC 11			
	intel -	Performance Kit, Intel(R) NUC 11 Performance Mini PC, Intel(R)			
	nuc_13_extreme_c	NUC Compute Element, Intel(R) NUC Laptop Kit, Intel(R) NUC Pro			
	ompute_element_	Kit, Intel(R) NUC Pro Board and Intel(R) NUC Pro Mini PC BIOS			
	nuc13sbbi7f_firmw	firmware may allow a privileged user to potentially enable			
CVE-2023-22444	are	information disclosure via local access.	2023-08-11	4.4	Medium
		Incorrect default permissions in the Intel(R) Support android			
		application before version v23.02.07 may allow a privileged user to			
CVE-2023-27392	intel - support	potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
	intel -	,			
	nuc_11_pro_kit_nu	Improper initialization in BIOS firmware for some Intel(R) NUCs			
	c11tnhi70z_firmwa	may allow a privileged user to potentially enable information			
CVE-2023-27887	re	disclosure via local access.	2023-08-11	4.4	Medium
<u> </u>		Unchecked return value in some Intel(R) RealSense(TM) ID			
	intel -	software for Intel(R) RealSense(TM) 450 FA in version 0.25.0 may			
	realsense_450_fa_f	allow a priviledged user to potentially enable denial of service via			
CVE-2023-29243	irmware	local access.	2023-08-11	4.4	Medium
<u> </u>	intel -	10001 0000001	2023 00 11	TT	ivicalulli
	nuc_11_performan	Exposure of sensitive information to an unauthorized actor in BIOS			
	ce_kit_nuc11pahi7	firmware for some Intel(R) NUCs may allow a privilege user to			
CVE-2023-29500	Oz_firmware	potentially enable information disclosure via local access.	2023-08-11	4.4	Medium
<u> </u>	intel -	Improper access control in some Intel(R) NUC BIOS firmware may	2023 00-11	7.7	ivicululli
	nuc_kit_nuc6cayh_	allow a privileged user to potentially enable denial of service via			
CVE-2023-32285	firmware	local access.	2023-08-11	4.4	Medium
CVL-2023-32203	iiiiiwale	An issue was discovered in Samsung NFC S3NRN4V, S3NSN4V,	2023-00-11	4.4	ivieululli
	cameuna				
CVE 2022 20402	samsung -	S3NSEN4, SEN82AB, and S3NRN82. A buffer copy without checking	2022 00 00	4.2	Madi
CVE-2023-36482	s3nrn4v_firmware	its input size can cause an NFC service restart.	2023-08-08	4.3	Medium
		Improper URL validation vulnerability in Samsung Members prior			
CVE 2022 20722	samsung -	to version 14.0.07.1 allows attackers to access sensitive	2022 00 10	4.0	N 41*
CVE-2023-30703	members	information.	2023-08-10	4.3	Medium
		Improper access control in Telecom prior to SMR Aug-2023			
0.45 0000 0000	samsung - multiple	Release 1 allows local attackers to call silenceRinger API without			
CVE-2023-30682	products	permission.	2023-08-10	3.3	Low
		Improper access control in Telecom prior to SMR Aug-2023			
	samsung - multiple	Release 1 allows local attackers to call endCall API without			
CVE-2023-30683	products	permission.	2023-08-10	3.3	Low
		Improper access control in Samsung Telecom prior to SMR Aug-			
	samsung - multiple	2023 Release 1 allows local attackers to call acceptRingingCall API			
CVE-2023-30684	products	without permission.	2023-08-10	3.3	Low
	samsung - multiple	Improper access control vulnerability in Telecom prior to SMR Aug-			
CVE-2023-30685	products	2023 Release 1 allows local attakcers to change TTY mode.	2023-08-10	3.3	Low
		PendingIntent hijacking vulnerability in SemWifiApTimeOutImpl in			
	samsung - multiple	framework prior to SMR Aug-2023 Release 1 allows local attackers			
CVE-2023-30700	products	to access ContentProvider without proper permission.	2023-08-10	3.3	Low
	1 1 2 2 2 2 2 2	The state of the 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.