

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

أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للتُغرات المسجلة vulnerabilities by the National Institute of Standards and Technology the National Institute of Standards and Technology (NIST) من قبل (NIST) National Vulnerability Database (NVD) for the week from 1st of .للأسبوع من ١ أبريل إلى ٨ أبريل إلى ٨ أبريل إلى ١ علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار April to 8th of April. Vulnerabilities are scored using the Common Common Vulnerability 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

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

عالى جدًا: النتيجة الأساسية لـCVSS 9.0-10.0

عالى: النتيجة الأساسية لـ8.9-CVSS 7.0

متوسط: النتيجة الأساسية لـ6.9-CVSS 4.0

منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
		IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are			
		vulnerable to a buffer overflow, caused by improper bounds			
	ibm - multiple	checking. An attacker could overflow a buffer and execute			
CVE-2023-27284	products	arbitrary code on the system. IBM X-Force ID: 248616.	2023-04-02	9.8	Critical
		IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are			
		vulnerable to a buffer overflow, caused by improper bounds			
	ibm - multiple	checking. An attacker could overflow a buffer and execute			
CVE-2023-27286	products	arbitrary code on the system. IBM X-Force ID: 248616.	2023-04-02	9.8	Critical
	jenkins - role-	Jenkins Role-based Authorization Strategy Plugin			
	based_authorizatio	587.v2872c41fa_e51 and earlier grants permissions even after			
CVE-2023-28668	n_strategy	they've been disabled.	2023-04-02	9.8	Critical
		Jenkins Convert To Pipeline Plugin 1.0 and earlier uses basic string			
		concatenation to convert Freestyle projects' Build Environment,			
		Build Steps, and Post-build Actions to the equivalent Pipeline step			
		invocations, allowing attackers able to configure Freestyle projects			
	jenkins -	to prepare a crafted configuration that injects Pipeline script code			
	convert_to_pipelin	into the (unsandboxed) Pipeline resulting from a convertion by			_
CVE-2023-28677	е	Jenkins Convert To Pipeline Plugin.	2023-04-02	9.8	Critical
	_	A pre-auth command injection vulnerability in the warn-proceed			
	sophos -	handler of Sophos Web Appliance older than version 4.3.10.4			_
CVE-2023-1671	web_appliance	allows execution of arbitrary code.	2023-04-04	9.8	Critical
		An issue was discovered in Samsung Exynos Mobile Processor and			
		Baseband Modem Processor for Exynos 1280, Exynos 2200, and			
	samsung -	Exynos Modem 5300. An integer overflow in IPv4 fragment			
	exynos_1280_firm	handling can occur due to insufficient parameter validation when			_
CVE-2023-28613	ware	reassembling these fragments.	2023-04-04	9.8	Critical
		A vulnerability in the web-based management interface of Cisco			
		RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN			
		Routers could allow an unauthenticated, remote attacker to			
		upload arbitrary files to an affected device. This vulnerability is due			
		to insufficient authorization enforcement mechanisms in the			
		context of file uploads. An attacker could exploit this vulnerability			
		by sending a crafted HTTP request to an affected device. A			
CVE 2022 20072	cisco -	successful exploit could allow the attacker to upload arbitrary files to the affected device.	2022 04 05	0.0	Cuitinal
CVE-2023-20073	rv340_firmware	** UNSUPPORTED WHEN ASSIGNED ** A Java insecure	2023-04-05	9.8	Critical
		deserialization vulnerability in Adobe LiveCycle ES4 version 11.0 and earlier allows unauthenticated remote attackers to gain			
		operating system code execution by submitting specially crafted			
		, , ,			
		Java serialized objects to a specific URL. Adobe LiveCycle ES4			
		version 11.0.1 and later may be vulnerable if the application is installed with Java environment 7u21 and earlier. Exploitation of			
		the vulnerability depends on two factors: insecure deserialization			
		methods used in the Adobe LiveCycle application, and the use of			
		Java environments 7u21 and earlier. The code execution is			
		performed in the context of the account that is running the Adobe			
	adobe -	LiveCycle application. If the account is privileged, exploitation			
CVE-2023-28500	livecycle_es4	provides privileged access to the operating system. NOTE: This	2023-04-06	9.8	Critical
CVL 2023 20300	IIVECYCIC_E34	provides privileged decess to the operating system. NOTE. 11115	2023 04-00	7.0	Citical

		vulnerability only affects products that are no longer supported by the maintainer.			
		Improper Control of Generation of Code ('Code Injection')			
	apache -	vulnerability in Apache Software Foundation Apache Airflow Hive			
	airflow_hive_provi	Provider.This issue affects Apache Airflow Hive Provider: before			
CVE-2023-28706	der	6.0.0.	2023-04-07	9.8	Critica
		A cross-site request forgery (CSRF) vulnerability in Jenkins			
	jenkins -	OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows			
	octoperf_load_testi	attackers to connect to a previously configured Octoperf server			
CVE-2023-28674	ng	using attacker-specified credentials.	2023-04-02	8.8	High
		A cross-site request forgery (CSRF) vulnerability in Jenkins Convert			
	jenkins -	To Pipeline Plugin 1.0 and earlier allows attackers to create a			
CVE 2022 20676	convert_to_pipelin	Pipeline based on a Freestyle project, potentially leading to	2022 04 02	0.0	Hiah
CVE-2023-28676	e	remote code execution (RCE).	2023-04-02	8.8	High
		Heap buffer overflow in Visuals in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who had compromised			
		the renderer process to potentially exploit heap corruption via a			
CVE-2023-1810	google - chrome	crafted HTML page. (Chromium security severity: High)	2023-04-04	8.8	High
<u>CVL 2023 1010</u>	googie emonie	Use after free in Frames in Google Chrome prior to 112.0.5615.49	2023 04 04	0.0	111611
		allowed a remote attacker who convinced a user to engage in			
		specific UI interaction to potentially exploit heap corruption via a			
CVE-2023-1811	google - chrome	crafted HTML page. (Chromium security severity: High)	2023-04-04	8.8	High
012 2020 2022	google emonie	Out of bounds memory access in DOM Bindings in Google Chrome	2020 0 . 0 .	0.0	
		prior to 112.0.5615.49 allowed a remote attacker to perform out			
		of bounds memory access via a crafted HTML page. (Chromium			
CVE-2023-1812	google - chrome	security severity: Medium)	2023-04-04	8.8	High
		Use after free in Networking APIs in Google Chrome prior to			5
		112.0.5615.49 allowed a remote attacker who convinced a user to			
		engage in specific UI interaction to potentially exploit heap			
		corruption via a crafted HTML page. (Chromium security severity:			
CVE-2023-1815	google - chrome	Medium)	2023-04-04	8.8	High
		Use after free in Vulkan in Google Chrome prior to 112.0.5615.49			
		allowed a remote attacker to potentially exploit heap corruption			
CVE-2023-1818	google - chrome	via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	8.8	High
		Heap buffer overflow in Browser History in Google Chrome prior to			
		112.0.5615.49 allowed a remote attacker who convinced a user to			
		engage in specific UI interaction to potentially exploit heap			
		corruption via a crafted HTML page. (Chromium security severity:			
CVE-2023-1820	google - chrome	Medium)	2023-04-04	8.8	High
		A vulnerability in the web-based management interface of Cisco			
		Secure Network Analytics could allow an authenticated, remote			
		attacker to execute arbitrary code on the underlying operating			
		system. This vulnerability is due to insufficient sanitization of user-			
		provided data that is parsed into system memory. An attacker			
	-:	could exploit this vulnerability by sending a crafted HTTP request			
	cisco -	to an affected device. A successful exploit could allow the attacker			
CVE 2022 20102	secure_network_an	to execute arbitrary code on the underlying operating system as	2022 04 05	0.0	High
CVE-2023-20102	alytics	the administrator user.	2023-04-05	8.8	High
	jenkins -	Jenkins Visual Studio Code Metrics Plugin 1.7 and earlier does not configure its XML parser to prevent XML external entity (XXE)			
CVE-2023-28681	visual_studio_code metrics	attacks.	2023-04-02	8.2	⊔iah
VE-2023-20001	jenkins -	Jenkins Performance Publisher Plugin 8.09 and earlier does not	2023-04-02	0.2	High
	performance_publi	configure its XML parser to prevent XML external entity (XXE)			
VE-2023-28682	sher	attacks.	2023-04-02	8.2	High
.VL-2023-20002	jenkins -	Jenkins Phabricator Differential Plugin 2.1.5 and earlier does not	2023-04-02	0.2	iligi
	phabricator_differe	configure its XML parser to prevent XML external entity (XXE)			
CVE-2023-28683	ntial	attacks.	2023-04-02	8.2	High
	ibm -	IBM Sterling Order Management 10.0 could allow a user to bypass	_525 57 52	5.2	811
	sterling_order_man	validation and perform unauthorized actions on behalf of other			
CVE-2022-33959	agement	users. IBM X-Force ID: 229320.	2023-04-07	8.1	High
		Apache James server version 3.7.3 and earlier provides a JMX			
		management service without authentication by default. This			
		allows privilege escalation by a malicious local user. Administrators			
		are advised to disable JMX, or set up a JMX password. Note that			
		version 3.7.4 onward will set up a JMX password automatically for			
CVE-2023-26269	apache - james	Guice users.	2023-04-03	7.8	High
		A vulnerability exists in Trellix Agent for Windows version 5.7.8			
		and earlier, that allows local users, during install/upgrade			
		workflow, to replace one of the Agent's executables before it can			
CVE-2023-0975	trellix - agent	be executed. This allows the user to elevate their permissions.	2023-04-03	7.8	High
		Heap based buffer overflow in binutils-gdb/bfd/libbfd.c in			
CVE-2023-1579	gnu - binutils	bfd_getl64.	2023-04-03	7.8	High
		Dell PowerScale OneFS version 9.5.0.0 contains improper link			
	1	resolution before file access vulnerability in isi_gather_info. A low			
				Ì	
	dell -	privilege local attacker could potentially exploit this vulnerability,			
	dell - emc_powerscale_o	privilege local attacker could potentially exploit this vulnerability, leading to system takeover and it breaks the compliance mode			
CVE-2023-25940		leading to system takeover and it breaks the compliance mode guarantees.	2023-04-04	7.8	High
CVE-2023-25940	emc_powerscale_o	leading to system takeover and it breaks the compliance mode	2023-04-04	7.8	High

	T				
		potentially exploit this vulnerability, leading to Denial of service,			
		escalation of privileges, and information disclosure. This			
		vulnerability breaks the compliance mode guarantee.			
		Multiple vulnerabilities in the restricted shell of Cisco Evolved			
		Programmable Network Manager (EPNM), Cisco Identity Services			
		Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to escape the restricted shell and			
	cisco -	gain root privileges on the underlying operating system. For more			
	identity_services_e	information about these vulnerabilities, see the Details section of			
CVE-2023-20122	ngine	this advisory.	2023-04-05	7.8	High
<u> </u>	ingine .	In mmsdk, there is a possible escalation of privilege due to a parcel	2023 0 1 03	7.10	6
		format mismatch. This could lead to local code execution with no			
		additional execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation. Patch ID: ALPS07203022; Issue ID:			
CVE-2023-20655	products	ALPS07203022.	2023-04-06	7.8	High
	·	Dell Power Manager, versions 3.10 and prior, contains an			
		Improper Access Control vulnerability. A low-privileged attacker			
	dell -	could potentially exploit this vulnerability to elevate privileges on			
CVE-2023-28051	power_manager	the system.	2023-04-07	7.8	High
		Jenkins Crap4J Plugin 0.9 and earlier does not configure its XML			
CVE-2023-28680	jenkins - crap4j	parser to prevent XML external entity (XXE) attacks.	2023-04-02	7.5	High
		mod_auth_openidc is an authentication and authorization module			
		for the Apache 2.x HTTP server that implements the OpenID			
		Connect Relying Party functionality. In versions 2.0.0 through			
		2.4.13.1, when 'OIDCStripCookies' is set and a crafted cookie			
		supplied, a NULL pointer dereference would occur, resulting in a			
		segmentation fault. This could be used in a Denial-of-Service			
		attack and thus presents an availability risk. Version 2.4.13.2			
01/2 0000 0	apache -	contains a patch for this issue. As a workaround, avoid using	2005 5 -		
CVE-2023-28625	http_server	`OIDCStripCookies`.	2023-04-03	7.5	High
		A vulnerability in the Vector Packet Processor (VPP) of Cisco Packet			
		Data Network Gateway (PGW) could allow an unauthenticated,			
		remote attacker to stop ICMP traffic from being processed over an			
		IPsec connection. This vulnerability is due to the VPP improperly			
		handling a malformed packet. An attacker could exploit this			
	oisaa	vulnerability by sending a malformed Encapsulating Security			
	cisco - packet_data_netw	Payload (ESP) packet over an IPsec connection. A successful exploit			
CVE-2023-20051		could allow the attacker to stop ICMP traffic over an IPsec connection and cause a denial of service (DoS).	2023-04-05	7.5	Hiαh
CVE-2023-20031	ork_gateway	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone	2023-04-03	7.5	High
	zohocorp - multiple	to conduct a Denial-of-Service attack via the Mobile App			
CVE-2023-28342	products	Authentication API.	2023-04-05	7.5	High
CVL 2023 20342	ibm -	IBM Sterling Order Management 10.0 does not require that users	2023 04 03	7.5	111611
	sterling_order_man	should have strong passwords by default, which makes it easier for			
CVE-2022-34333	agement	attackers to compromise user accounts. IBM X-Force ID: 229698.	2023-04-07	7.5	High
<u> </u>	apache -	Improper Input Validation vulnerability in Apache Software	2020 0 1 07	7.15	6
	airflow_drill_provid	Foundation Apache Airflow Drill Provider. This issue affects Apache			
CVE-2023-28707	er	Airflow Drill Provider: before 2.3.2.	2023-04-07	7.5	High
	apache -	Improper Input Validation vulnerability in Apache Software		_	<u> </u>
	airflow_spark_prov	Foundation Apache Airflow Spark Provider. This issue affects			
CVE-2023-28710	ider	Apache Airflow Spark Provider: before 4.0.1.	2023-04-07	7.5	High
		A post-auth command injection vulnerability in the exception			
	sophos -	wizard of Sophos Web Appliance older than version 4.3.10.4			
CVE-2022-4934	web_appliance	allows administrators to execute arbitrary code.	2023-04-04	7.2	High
		A vulnerability in the web-based management interface of Cisco			
		Small Business RV016, RV042, RV042G, RV082, RV320, and RV325			
		Routers could allow an authenticated, remote attacker to execute			
		arbitrary commands on an affected device. This vulnerability is due			
		to improper validation of user input within incoming HTTP packets.			
		An attacker could exploit this vulnerability by sending a crafted			
		HTTP request to the web-based management interface. A			
		successful exploit could allow the attacker to gain root-level			
		privileges and access unauthorized data. To exploit this			
		vulnerability, an attacker would need to have valid administrative			
	cisco -	credentials on the affected device. Cisco has not released software			
CVE-2023-20124	rv016_firmware	updates that address this vulnerability.	2023-04-05	7.2	High
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN			
		Routers could allow an authenticated, remote attacker to inject			
		and execute arbitrary commands on the underlying operating			
		system of an affected device. These vulnerabilities are due to			
		insufficient validation of user-supplied input. An attacker could			
		exploit these vulnerabilities by sending malicious input to an			
		affected device. A successful exploit could allow the attacker to			
		execute arbitrary commands as the root user on the underlying			
		Linux operating system of the affected device. To exploit these			
	_:	vulnerabilities, an attacker would need to have valid Administrator			
CVE 2022 20422	cisco -	credentials on the affected device. Cisco has not released software	2022 04 05	7.3	<u> </u>
CVE-2023-20128	rv320_firmware	updates to address these vulnerabilities.	2023-04-05	7.2	High

		A vulnerability in Cisco Secure Network Analytics could allow an			
		authenticated, remote attacker to execute arbitrary code as a root			
		user on an affected device. This vulnerability is due to insufficient			
		validation of user input to the web interface. An attacker could			
		exploit this vulnerability by uploading a crafted file to an affected			
	-:	device. A successful exploit could allow the attacker to execute			
	cisco -	code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the			
CVE-2023-20103	secure_network_an alytics	affected device.	2023-04-05	7.2	High
CVL-2023-20103	alytics	Multiple vulnerabilities in the web-based management interface of	2023-04-03	1.2	Iligii
		Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN			
		Routers could allow an authenticated, remote attacker to inject			
		and execute arbitrary commands on the underlying operating			
		system of an affected device. These vulnerabilities are due to			
		insufficient validation of user-supplied input. An attacker could			
		exploit these vulnerabilities by sending malicious input to an			
		affected device. A successful exploit could allow the attacker to			
		execute arbitrary commands as the root user on the underlying			
		Linux operating system of the affected device. To exploit these			
		vulnerabilities, an attacker would need to have valid Administrator			
	cisco -	credentials on the affected device. Cisco has not released software			_
CVE-2023-20117	rv320_firmware	updates to address these vulnerabilities.	2023-04-05	7.2	High
		A use-after-free flaw was found in vhost_net_set_backend in			
		drivers/vhost/net.c in virtio network subcomponent in the Linux			
		kernel due to a double fget. This flaw could allow a local attacker			
CVE_2022 1020	linuv - linuv komal	to crash the system, and could even lead to a kernel information	2022 04 05	71	Lich
CVE-2023-1838	linux - linux_kernel	leak problem. Dell Display Manager, versions 2.1.0 and prior, contains an	2023-04-05	7.1	High
		arbitrary file or folder deletion vulnerability during uninstallation A			
		local low privilege attacker could potentially exploit this			
	dell -	vulnerability, leading to the deletion of arbitrary files on the			
CVE-2023-28046	display_manager	operating system with high privileges.	2023-04-06	7.1	High
		IBM TRIRIGA 4.0 is vulnerable to an XML external entity injection			
	ibm -	(XXE) attack when processing XML data. A remote attacker could			
	tririga_application_	exploit this vulnerability to expose sensitive information or			
CVE-2023-27876	platform	consume memory resources. IBM X-Force ID: 249975.	2023-04-07	7.1	High
		Multiple vulnerabilities in specific Cisco Identity Services Engine			
		(ISE) CLI commands could allow an authenticated, local attacker to			
		perform command injection attacks on the underlying operating			
		system and elevate privileges to root. To exploit these			
		vulnerabilities, an attacker must have valid Administrator			
		privileges on the affected device. These vulnerabilities are due to			
		insufficient validation of user-supplied input. An attacker could			
	cisco -	exploit these vulnerabilities by submitting a crafted CLI command.			
CVE-2023-20021	identity_services_e	A successful exploit could allow the attacker to elevate privileges	2023-04-05	6.7	Medium
UVE-2023-20021	ngine	to root. Multiple vulnerabilities in specific Cisco Identity Services Engine	2023-04-03	0.7	Medium
		(ISE) CLI commands could allow an authenticated, local attacker to			
		perform command injection attacks on the underlying operating			
		system and elevate privileges to root. To exploit these			
		vulnerabilities, an attacker must have valid Administrator			
		privileges on the affected device. These vulnerabilities are due to			
		insufficient validation of user-supplied input. An attacker could			
	cisco -	exploit these vulnerabilities by submitting a crafted CLI command.			
	1				
CVE 2022 20022	identity_services_e	A successful exploit could allow the attacker to elevate privileges			
CVE-2023-20022	ngine	A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
<u> </u>		to root. Multiple vulnerabilities in specific Cisco Identity Services Engine	2023-04-05	6.7	Medium
<u> </u>		to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to	2023-04-05	6.7	Medium
<u>CVE-2023-20022</u>		to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating	2023-04-05	6.7	Medium
<u>LVE-2023-20022</u>		to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these	2023-04-05	6.7	Medium
<u>CVE-2023-20022</u>		to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator	2023-04-05	6.7	Medium
<u>CVE-2023-20022</u>		to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to	2023-04-05	6.7	Medium
<u>CVE-2023-20022</u>	ngine	to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could	2023-04-05	6.7	Medium
<u>CVE-2023-20022</u>	ngine cisco -	to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command.	2023-04-05	6.7	Medium
	cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges			
	ngine cisco -	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
	cisco - identity_services_e	to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine			
	cisco - identity_services_e	to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to			
	cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating			
	cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these			
CVE-2023-20022	cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator			
	cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to			
	cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator			
	cisco - identity_services_e ngine	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could			
CVE-2023-20023	cisco - identity_services_e ngine cisco -	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command.			
CVE-2023-20023	cisco - identity_services_e ngine cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges	2023-04-05	6.7	Medium
	cisco - identity_services_e ngine cisco - identity_services_e	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
CVE-2023-20023	cisco - identity_services_e ngine cisco - identity_services_e	to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root. Multiple vulnerabilities in the restricted shell of Cisco Evolved	2023-04-05	6.7	Medium

information about these vulnerabilities, see the petalis section of the advisory. Multiplie vulnerabilities in specific Coco identity Services Frigine Wild value of the petalists of the underlying operating vulnerabilities and could allow an authoristicate local statistical roperating vulnerabilities and set on the underlying operating vulnerabilities and with the underlying operating vulnerabilities and vulnerabilities are due to interest on the operation of privilege with System execution privileges and privileges vulnerabilities and vulnerabilities and vulnerabilities and vulnerabilities and vulnerabilities and vulnerabilities and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to interest on the control and vulnerabilities are due to a final vulnerabilities. And vulnerabilities are due to a final vulnerabilities are due to a final vulnerabilities. And vulnerabilities are due to a final vulnerabilities are due to a final vulnerabilities. And vulnerabilities are due to a final vulnerabilities are due to a final vulnerabilities. And vulnerabilities ar		1				Ι
Mistiple vulnerabilities in specific Cisco identity Services Engine (ISE) CLI commands could allow an authenticated. Incal attacker to perform command incelled an authenticated. Incapitation of the commands could allow an authenticated in capitation of the commands could allow an authenticated. Incapitation of the commands could allow an authenticated in the commands of the comma			gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of			
Multiple witherabilities in specific Cisco tentity Services Engine (SIC) L1 command out all allow an utacks on the underlying operating system and elevers bridges to note. To export these vulnerabilities, an attacks not the underlying operating system and elevers bridges to note. To export these vulnerabilities, an attacker may be reported to the command injection attacks on the underlying operating system and elevers bridges for note. To export these vulnerabilities, an attacker may be reported to the command. As a curseful application of the command of						
perform command injection attacks on the underlying operating system and eleviser privileges on the part Privilege with special interval death infinition or supering the entire of the privilege and the affected devere. These undershifteds are due to insufficient validation of user-pupplied injust. An attacker could identify, carvices, e. societies and public could allow the stocker to elevise privilege. The products in privilege with special products are could injust the stocker to elevise privilege with system execution privilege receids. Der interaction is not needed for exploitation Patrix ID: ALPSO766390; bissue ID: ALPSO766390. ALPSO7628165; issue ID: ALPSO7969390; bissue ID: ALPSO769390. ALPSO7628165; issue ID: ALPSO7969390; bissue ID: ALPSO7969990; bissue ID: ALPSO796990; bis			,			
system and devote privileges to root. To exploit these vulnerabilities are due to privileges on the affected device. These vulnerabilities are due to privileges on the affected device. These vulnerabilities are due to privileges on the affected device. These vulnerabilities are due to privilege on the affected device. These vulnerabilities are due to incompany the privilege of			(ISE) CLI commands could allow an authenticated, local attacker to			
villears billings, an attacker must have valid Administratory privileges on the diffected device. Preve valientabilities are due to insufficient validation of user-supplied input. An attacker could exploit three vulnerabilities by submiting a carted of Loromand. A successful exploit could allow the attacker to device privilege to root. In rpmb, tracellar products google - multiple products produc			, , , , , , , , , , , , , , , , , , , ,			
privileges on the affected device. These vulnerabilities are due to insufficient validation of user supplied input. An statistic round exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit to found white due to a bloic interest of the products of the products. In products of the pro			, -			
cisco— insufficient validation of user-supplied input. An attacker could explore the explore these value rabilities by submitting a carted CU command. A successful exploit could allow the attacker to elevate privilege to root. In pmit, there is a possible out of bounds write due to a logic product. In pmit, there is a possible out of bounds write due to a logic product. In product in the product in the product in the pmit product in the product in the pmit product in the product						
cur-2023-20131 of certainty_services_ a successful exploit could allow the tacker to delevate privileges by a successful exploit could allow the tacker to delevate privileges by a successful exploit could allow the tacker to delevate privileges by a successful exploit could allow the tacker to delevate privileges with System geogle - multiple products by a successful exploit privilege with System execution privileges needed. Liver interaction is not needed for exploitation. Patch 110: All PS07460390, Bisue ID. All PS07460390, Bisue ID. All PS07460390. WE 2023-20652 products products a liver product by a successful privilege with System association privileges medical bear of privileges and special privi			'			
USE 2023-20153 VE 2023-20154 VE 2023-20155 VE 20		cisco -	· · · · ·			
The 2023-20153 night to root. 2023-04-05 6.7 Medium morth, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation. Parch ID: ALPS074603900; Issue ID: ALPS074603900. 2023-04-06 6.7 Medium me			· · · · · · · · · · · · · · · · · · ·			
In tymph, there is a possible out of bounds write due to a logic error. This could lead to local establishment of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch In J. AIRPS/0740998 (Sour ID. AIRPS/0740998). VE-2023-20652 products in keyintall, there is a possible out of bounds write due to a missing bounds check. This could lead to local establishment of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: AIRPS/0740989. VE-2023-20652 products in keyintall, there is a possible out of bounds write due to a missing bounds check. This could lead to local establishment of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: AIRPS/0748188, Issue ID. AIRPS/0748184. VE-2023-20653 products in Reymitall, there is a possible out of bounds write due to a missing bounds check. This could lead to local establishment of privilege with System execution privileges exceeded. User interaction is not needed for exploitation. Patch ID: AIRPS/0748188, Issue ID. AIRPS/07489184. VE-2023-20654 products in System execution privileges needed. User interaction is a for needed for exploitation. Patch ID: AIRPS/0748188, Issue ID. AIRPS/07489184. Legopiele multiple products in the products of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: AIRPS/0748184, Issue ID: AIRPS/07484, Issue ID: AIRPS/0748184, Issue ID: AIRPS/07484, Issue ID: AIRPS/0748184, Issue ID	CVE-2023-20153	·		2023-04-05	6.7	Medium
ver. 2023 23599 google - multiple products privileges meeded. User interaction is not needed for products in exploitation. Patch 10: ALPS97024999 (Susue ID. ALPS970249039). 2023-04-06 6.7 Medium missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch 10: ALPS97028188, Issue ID: ALPS97028188. Issue ID: ALPS97028189. Issue ID:			In rpmb, there is a possible out of bounds write due to a logic			
vv. 2023.2059 products exploitation. Patch ID: ARISPO7460390; base ID: AIPSO7460390. 2023.04.06 6.7 Medium in Reynitati, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege medium interaction is not needed for exploitation. Patch ID: AIPSO726186; stere ID: AIPSO7801818. 2023.04.06 6.7 Medium interaction is not needed for exploitation. Patch ID: AIPSO726186; stere ID: AIPSO7801818. 2023.04.06 6.7 Medium interaction is not needed for exploitation. Patch ID: AIPSO726186; stere ID: AIPSO780186. 2023.04.06 6.7 Medium interaction is not needed for exploitation. Patch ID: AIPSO780186; stere ID: AIPSO780186. Stere ID: AIP			error. This could lead to local escalation of privilege with System			
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 exploitation. Patch ID: ALPS07528168; Issue ID: ALPS07589135. VE 2023-20652 products 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 exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. VE 2023-20654 products interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. VE 2023-20654 products interaction is not needed for exploitation patch ID: ALPS07628168; Issue ID: ALPS07589146. VE 2023-20656 products interaction is not needed for exploitation patch ID: ALPS07628168; Issue ID: ALPS07589146. VE 2023-20656 products interaction is not needed for exploitation. Patch ID: ALPS075791485. VE 2023-20657 products interaction is not needed for exploitation. Patch ID: ALPS075791485. VE 2023-20658 products interaction is not needed for exploitation. Patch ID: ALPS075791485. VE 2023-20659 products interaction is not needed for exploitation. Patch ID: ALPS07579485; Issue ID: ALPS07579485. VE 2023-20659 products interaction is not needed for exploitation. Patch ID: ALPS07579485; Issue ID: ALPS07579485. VE 2023-20669 products interaction is not needed for exploitation. Patch ID: ALPS07579485; Issue ID: ALPS075894848. VE 2023-20669 products interaction provides needed. User interaction is not needed for exploitation. Patch ID: ALPS075893938; Issue ID: ALPS075894848. VE 2023-20669 products interaction provides needed. User interaction is not needed for exploitation. Patch ID: ALPS075893938; Issue ID: ALPS075895848. VE 2023-20669 products interaction provides needed. User interaction is not needed for exploitation. Patch ID: ALPS075897895; Issue ID: ALPS075897894; Issue ID: ALPS0758978941; Issue ID: ALPS075899			, -			
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: APS07628186, Issue ID: APS07628186. VE-2023-20653 products 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 exploitation. Patch ID: APS07628186, Issue ID: APS07589184. VE-2023-20654 products 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 exploitation. Patch ID: APS07628186, Issue ID: APS07598148. VE-2023-20654 products In genicone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: APS07628186; Issue ID: APS075798148. VE-2023-20652 products In mee, there is a possible out of bounds write due to a logic exploitation. Patch ID: APS07678194, Issue ID: APS07577149. VE-2023-20652 products In mee, 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: APS07578185, Issue ID: APS07781945. VE-2023-20652 products In sp. 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: APS07580783, Issue ID: APS07580782. VE-2023-20652 products In sp. 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 nee	CVE-2022-32599	products		2023-04-06	6.7	Medium
opage -multiple VE-2023-20652 VE-2023-20653 VE-2023-20654 VE-2023-20656 VE-2023-20656 VE-2023-						
ver. 2023-20652 Ver. 2023-20652 Ver. 2023-20653 ver. 2023-20653 ver. 2023-20653 ver. 2023-20653 ver. 2023-20654 ver. 2023-20654 ver. 2023-20655 ver. 2023-20655 ver. 2023-20656 ver. 2023-20657 ver. 2023-20657 ver. 2023-20657 ver. 2023-20658 ver. 2023-20658 ver. 2023-20659 ver. 2023-20669 ver. 2						
VE-2023-20652 products APS07628188, Issue ID: AIPS07589145. 2023-04-06 6.7 Medium 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 exploitation. Patch ID: AIPS07628188, Issue ID: AIPS07628189, Issue ID: AIPS076288189, Issue ID: AIPS076288189, Issue ID: AIPS076288189, Issue ID: AIPS076288189, Issue ID: AIPS076888189, Issue ID: AIPS07686819, Issue ID: AIPS07686969, Issue ID: AIPS0766069, I		google - multiple	, , , , , , , , , , , , , , , , , , , ,			
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 exploitation. Parch ID: ALPS07823168; Issue ID: ALPS07829144. VE-2023-20654 VE-2023-20654 VE-2023-20655 VE-2023-20656 VE-2023-20657 VE-2023-20658 In Issue ID: ALPS078251485 In Issue ID: ALPS078251494 In Instantial Ins	CVF-2023-20652		·	2023-04-06	6.7	Medium
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/07528168; Issue ID. APS/07528144. Discription of the products		p: 00:0:0	·			
Section						
### APSO/528168; Issue ID: ALPSO/528144. ### APSO/528168; Issue ID: ALPSO/528146. ### 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 exploitation. Patch ID: ALPSO/528168; Issue ID: ALPSO/528148. #### APSO/528168; Issue ID: ALPSO/5281494; Issue ID: ALPSO/5281494. #### APSO/528168; Issue ID: ALPSO/5281494; Issue ID: ALPSO/5281494. #### APSO/528168; Issue ID: ALPSO/5281494; Issue ID: ALPSO/5281494. #### APSO/528149. #### APSO/528149. #### ALPSO/528149. #### APSO/528149.			privilege with System execution privileges needed. User			
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 exploitation, Patch ID. ALPS/07628168, Issue ID: ALPS/07589148. In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS/075891494. In mittee, 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/07571498, such ID: ALPS/07571498. VE-2023-20657 In mittee, 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/07571485, Issue ID: ALPS/07571485. VE-2023-20658 VE-2023-20659 In wan, 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/07537393; Issue ID: ALPS/07580596. In wan, 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/07580782; Issue ID: ALPS/07580782. ALPS/07580782. In wan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS/07580782; Issue ID: ALPS/07580782. In wan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of priv		google - multiple	interaction is not needed for exploitation. Patch ID:			
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: APS075288413; In whan, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS075781494, Issue ID: ALPS075781494, Issue ID: ALPS075781494, Issue ID: ALPS07571494, Issue ID: ALPS0758413, Issue ID: ALPS0758413, Issue ID: ALPS0758413, Issue ID: ALPS07588413, Issue ID: ALPS075860782, Issue ID: ALPS07580782, Issue ID: ALPS075807932, Issue ID: ALPS075807932, Issue ID: ALPS075807932, Issue ID: ALPS075807932, Issue ID: ALPS	CVE-2023-20653	products	ALPS07628168; Issue ID: ALPS07589144.	2023-04-06	6.7	Medium
privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: Description Privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID:						
products APS07623186; Issue Dr. APS07539189. VE-2023-20656 Products In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS075371494; Issue ID: ALPS07571494; Issue ID: ALPS07571495; Issue ID: ALPS07571496; Issue ID: ALPS07571496; Issue ID: ALPS07571496; Issue ID: ALPS07571496; Issue ID: ALPS075607785; Issue ID:						
Products APS07628168; Issue ID: APS07589148. APS07628168; Issue ID: APS07589148. In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for google - multiple google - multiple products APS07571494. APS07571494; Issue ID: APS07571494. In mete, 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: APS07571495; Issue ID: APS07571495. APS07571485; Issue ID: APS07180396. APS07180396. In what, 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: APS07588413; Issue ID: APS07588413. In what, 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: APS07588413; Issue ID: APS07588413. In what, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: APS07560782; Issue ID: APS07560782. In what, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: APS07560785; Issue ID: APS07560741. In what, there is a possible out of bounds write due t		annala manikinia				
In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. 2023-04-06 6.7 Mediun products products and products are products. In interact, the products are products. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. In is, p. 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: ALPS0757393; Issue ID: ALPS0757180396. Description of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07537933; Issue ID: ALPS075780396. Description of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS0758843; Issue ID: ALPS07588413. Issue ID: ALPS07388413. Issue	CVE 2022 20654		·	2022 04 06	6.7	Modium
error. This could lead to local escalation of privilege with System google - multiple products VE-2023-20656	CVE-2023-20034	products		2023-04-00	0.7	Medium
products pro			The state of the s			
Experiment Exp		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: ALPSO7571485; Issue ID: ALPSO7571485. In isp, 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: ALPSO7589393; Issue ID: ALPSO7180396. ZVE-2023-20658 products In wlan, 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: ALPSO7588413; Issue ID: ALPSO75888413. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO75860782; Issue ID: ALPSO7580782. ALPSO7580782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7560782; Issue ID: ALPSO7560782. ALPSO7560782. ALPSO7560783. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges meeded. User interaction is not needed for exploitation. Patch ID: ALPSO7560765; Issue ID: ALPSO7560765. ALPSO75	CVE-2023-20656		, ,	2023-04-06	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7571485, Issue ID: 2023-04-06 6.7 Mediun In isp, 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: ALPSO7537393; Issue ID: 2023-04-06 6.7 Mediun In wlan, 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: ALPSO758393; Issue ID: 2023-04-06 6.7 Mediun In wlan, 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: ALPSO7588413; Issue ID: 2023-04-06 6.7 Mediun In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7560782; Issue ID: 2023-04-06 6.7 Mediun In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges with System execution is not needed for exploitation. Patch ID: ALPSO7560741; Issue ID: 2023-04-06 6.7 Mediun In go, the reis a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7560759592. 2023-04-06 6.7 Mediun In		·	·			
Section			bounds check. This could lead to local escalation of privilege with			
In wan, 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: ALPS075807837393; issue ID: ALPS07180396. In wlan, 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: ALPS07588413; issue ID: ALPS07588413. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07580782; issue ID: ALPS07580782; issue ID: ALPS07560782; issue ID: ALPS07560792; issue ID: ALPS07560						
In isp, 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: ALPS075807393; Issue ID: ALPS07180396. In wlan, 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: ALPS07588413; Issue ID: ALPS07588413. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07580782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560755; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560755; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: AL			•			
bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07587393; Issue ID: ALPS07180396. In wlan, 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: ALPS07588413; Issue ID: ALPS07588413. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS075688413; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560761; Issue ID: ALPS07560761; Issue ID: ALPS07560741; Issue ID: ALPS075059592; Issue ID: ALPS075059592. In display drm, there is a possible dout 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: ALPS075059592; Issue ID: ALPS075059592; Issue ID: ALPS075059592; Issue ID: ALPS0779310651; Issue ID: ALPS0779	CVE-2023-20657	products		2023-04-06	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO75837393; Issue ID: ALPSO7580784. System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO758037393; Issue ID: ALPSO7580396. In wlan, 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: ALPSO7588413; Issue ID: ALPSO7588413. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7560782; Issue ID: ALPSO7560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO75607565; Issue ID: ALPSO7560785. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7560765; Issue ID: ALPSO7560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7560741; Issue ID: ALPSO7560741; Issue ID: ALPSO7560741; Issue ID: ALPSO7560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPSO7505952; Issue ID: ALPSO7505952. 2023-04-06 6.7 Mediun In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation o			· · ·			
google - multiple products needed for exploitation. Patch ID: ALPS07537393; Issue ID: ALPS07180396. 2023-04-06 6.7 Mediun			, -			
DVE-2023-20658 products ALPS07180396. In wlan, 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: ALPS07588413; Issue ID: ALPS075884313. 2023-04-06 6.7 Medium In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. 2023-04-06 6.7 Medium In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. 2023-04-06 6.7 Medium In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. 2023-04-06 6.7 Medium In with the system execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. 2023-04-06 6.7 Medium In In with the system execution privileges with System execution privileges with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS075607541. 2023-04-06 6.7 Medium In display drm, 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 with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS073505952. 2023-04-06 6.7 Medium In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of priv		google - multiple	,			
In wlan, 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: ALPS07588413; Issue ID: ALPS07588413. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. VE-2023-20661 In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765. 2023-04-06 6.7 Mediun In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS075050750741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges with System execution privileges with System execution privileges on the products In displaymon, 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: ALPS0731065	CVE-2023-20658			2023-04-06	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: ALPS07588413; Issue ID: ALPS07588413. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952. In display drm, 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: ALPS073030651; Issue ID: ALPS0730310651; Issue ID: ALPS073292173. In audio, 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: ALPS07310651; Iss		promote				
google - multiple products ALPSO7588413. 2023-04-06 6.7 Mediun						
ALPS07588413. 2023-04-06 6.7 Medium In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. 2023-04-06 6.7 Medium In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765; Issue ID: ALPS07560765; Issue ID: ALPS07560765. 2023-04-06 6.7 Medium In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. 2023-04-06 6.7 Medium In google - multiple products In In gr, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. 2023-04-06 6.7 Medium In display drm, 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: ALPS07310651; Issue ID: ALPS073292173. 2023-04-06 6.7 Medium In audio, 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 with System execution privilege with D: ALPS07310651; Issue ID: ALPS073292173. 2023-04-06 6.7 Medium In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation o						
In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560741; Issue ID: ALPS07560741. In wlan, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952, Issue ID: ALPS07505952. In display drm, 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 with System execution privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. ALPS07310651; Issue ID: ALPS072029173. ALPS07310651; Issue ID: ALPS072173. ALPS07306651; Issue ID: ALPS072173. AL		google - multiple	needed for exploitation. Patch ID: ALPS07588413; Issue ID:			
overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display dram, 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 with System execution privilege interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS0729173. ALPS07310651; Issue ID: ALPS07292173. In audio, 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 with System execution privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07329173. ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead	CVE-2023-20659	products		2023-04-06	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In google - multiple products In google - multiple products In google - multiple products In display drm, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS0750952; Issue ID: ALPS0750952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. In audio, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with			•			
google - multiple products needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. 2023-04-06 6.7 Medium			·			
December 2023-20661 Products ALPS07560782. 2023-04-06 6.7 Medium		annala manikinia	, ,			
In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS0730651; Issue ID: ALPS07302173. In audio, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, 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 with System execution privilege with System execution privilege sneeded. User interaction is not needed for exploitation. Patch ID: ALPS07304-06 6.7 Medium In audio, 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 with System execu	CVE_2022_20661			2022-04-06	6.7	Medium
overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. In audio, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	CVE-2023-20001	products		2023-04-00	0.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed. User interaction is not needed. User interaction is not needed for exploitation. Patch ID: ALPS07305952; Issue ID: ALPS07505952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with			·			
google - multiple products Reded for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. 2023-04-06 6.7 Medium			·			
In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. CVE-2023-20663		google - multiple	, ,			
overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	CVE-2023-20662	products	ALPS07560765.	2023-04-06	6.7	Medium
System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. 2023-04-06 6.7 Medium In display drm, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with			In wlan, there is a possible out of bounds write due to an integer			
google - multiple products ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Boogle - multiple products ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with			· · ·			
ALPS07560741. In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privileges needed. User interaction is not needed for exploitation. Boogle - multiple products ALPS07310651; Issue ID: ALPS07292173. In audio, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with			, ,			
In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, 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 with ID: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	CVE 2022 20002		•	2022 04 06	6.7	Na di di
could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing google - multiple google - multiple google - multiple bounds check. This could lead to local escalation of privilege with	CVE-2023-20663	products		2023-04-06	6.7	ivieaium
google - multiple privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with						
Patch ID: ALPS07505952; Issue ID: ALPS07505952. In display drm, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with		google - multinle				
In display drm, 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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	CVE-2023-20664		1, -	2023-04-06	6.7	Medium
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: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with		p. 23000		1_1 0.00		
privilege with System execution privileges needed. User google - multiple interaction is not needed for exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with			, , , , ,			
CVE-2023-20666 products ALPS07310651; Issue ID: ALPS07292173. 2023-04-06 6.7 Medium google - multiple bounds check. This could lead to local escalation of privilege with						
In audio, there is a possible out of bounds write due to a missing google - multiple bounds check. This could lead to local escalation of privilege with			· ·			
google - multiple bounds check. This could lead to local escalation of privilege with	CVE-2023-20666	products	·	2023-04-06	6.7	Medium
<u>_ve-2023-206/0</u> products System execution privileges needed. User interaction is not 2023-04-06 6.7 Mediun	C) /F 2022 2222		·	2022 24 22	c =	
	CVE-2023-20670	products	system execution privileges needed. User interaction is not	2023-04-06	6.7	Medium

		needed for exploitation. Patch ID: ALPS07648710; Issue ID:			
		ALPS07648710.			
		In adsp, there is a possible out of bounds write due to improper			
		input validation. This could lead to local escalation of privilege with			
	googlo multiple	System execution privileges needed. User interaction is not			
CVE-2023-20680	google - multiple products	needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785.	2023-04-06	6.7	Mediun
CVL-2023-20080	products	In adsp, there is a possible out of bounds write due to improper	2023-04-00	0.7	ivieului
		input validation. This could lead to local escalation of privilege with			
		System execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation. Patch ID: ALPS07696134; Issue ID:			
CVE-2023-20681	products	ALPS07696134.	2023-04-06	6.7	Mediur
		In wlan, there is a possible out of bounds write due to an integer			
		overflow. This could lead to local escalation of privilege with			
		System execution privileges needed. User interaction is not			
6) /5 2022 20602	google - multiple	needed for exploitation. Patch ID: ALPS07441605; Issue ID:	2022 04 06	6.7	na di
CVE-2023-20682	products	ALPS07441605. Jenkins OctoPerf Load Testing Plugin Plugin 4.5.1 and earlier does	2023-04-06	6.7	Mediun
		not perform a permission check in a connection test HTTP			
		endpoint, allowing attackers with Overall/Read permission to			
	jenkins -	connect to an attacker-specified URL using attacker-specified			
	octoperf_load_testi	credentials IDs obtained through another method, capturing			
CVE-2023-28672	ng ng	credentials stored in Jenkins.	2023-04-02	6.5	Mediun
		Jenkins remote-jobs-view-plugin Plugin 0.0.3 and earlier does not			
	jenkins - remote-	configure its XML parser to prevent XML external entity (XXE)			
CVE-2023-28684	jobs-view	attacks.	2023-04-02	6.5	Mediun
		A heap-based overflow vulnerability in Trellix Agent (Windows and			
		Linux) version 5.7.8 and earlier, allows a remote user to alter the			
CVE-2023-0977	trolliv agant	page heap in the macmnsvc process memory block resulting in the	2023-04-03	6.5	Madius
CVE-2023-0977	trellix - agent	service becoming unavailable. The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919	2023-04-03	6.5	Mediun
		Confidential attribute disclosure vi LDAP filters was insufficient and			
	samba - multiple	an attacker may be able to obtain confidential BitLocker recovery			
CVE-2023-0614	products	keys from a Samba AD DC.	2023-04-03	6.5	Mediun
	'	Dell PowerScale OneFS versions 8.2.x-9.4.x contain an			
		uncontrolled resource consumption vulnerability. A malicious			
	dell - multiple	network user with low privileges could potentially exploit this			
CVE-2023-25942	products	vulnerability in SMB, leading to a potential denial of service.	2023-04-04	6.5	Mediun
		Inappropriate implementation in Extensions in Google Chrome			
		prior to 112.0.5615.49 allowed an attacker who convinced a user			
0.45 2022 4042		to install a malicious extension to bypass file access restrictions via	2022 04 04	6.5	
CVE-2023-1813	google - chrome	a crafted HTML page. (Chromium security severity: Medium) Insufficient validation of untrusted input in Safe Browsing in	2023-04-04	6.5	Mediun
		Google Chrome prior to 112.0.5615.49 allowed a remote attacker			
		to bypass download checking via a crafted HTML page. (Chromium			
CVE-2023-1814	google - chrome	security severity: Medium)	2023-04-04	6.5	Mediun
<u> </u>	8008.0 00	Incorrect security UI in Picture In Picture in Google Chrome prior		0.0	
		to 112.0.5615.49 allowed a remote attacker to potentially perform			
		navigation spoofing via a crafted HTML page. (Chromium security			
CVE-2023-1816	google - chrome	severity: Medium)	2023-04-04	6.5	Mediun
		Insufficient policy enforcement in Intents in Google Chrome on			
		Android prior to 112.0.5615.49 allowed a remote attacker to			
		bypass navigation restrictions via a crafted HTML page. (Chromium			
CVE-2023-1817	google - chrome	security severity: Medium)	2023-04-04	6.5	Mediun
		Out of bounds read in Accessibility in Google Chrome prior to			
		112.0.5615.49 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium			
CVE-2023-1819	google - chrome	security severity: Medium)	2023-04-04	6.5	Mediur
CAT-5052-1012	googie - cilioffie	Inappropriate implementation in WebShare in Google Chrome	2023-04-04	0.5	ivieulun
		prior to 112.0.5615.49 allowed a remote attacker to potentially			
		hide the contents of the Omnibox (URL bar) via a crafted HTML			
CVE-2023-1821	google - chrome	page. (Chromium security severity: Low)	2023-04-04	6.5	Mediun
	- 5 - 5	Incorrect security UI in Navigation in Google Chrome prior to			
		112.0.5615.49 allowed a remote attacker to perform domain			
		spoofing via a crafted HTML page. (Chromium security severity:			
CVE-2023-1822	google - chrome	Low)	2023-04-04	6.5	Mediun
		Inappropriate implementation in FedCM in Google Chrome prior			
		to 112.0.5615.49 allowed a remote attacker to bypass navigation			
CVE 2022 1255		restrictions via a crafted HTML page. (Chromium security severity:	2022 21 2 -	c -	
CVE-2023-1823	google - chrome	Low)	2023-04-04	6.5	Mediun
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain			
		privileged information and conduct cross-site scripting (XSS) and			
	cisco - multinle	· · · · · · · · · · · · · · · · · · ·			
CVE-2023-20127	cisco - multiple products	cross-site request forgery (CSRF) attacks. For more information	2023-04-05	6.5	Mediun
CVE-2023-20127	cisco - multiple products	cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory.	2023-04-05	6.5	Mediun
CVE-2023-20127		cross-site request forgery (CSRF) attacks. For more information	2023-04-05	6.5	Medium

1		privileged information and annulus areas (1990)			<u> </u>
		privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information			
		about these vulnerabilities, see the Details section of this advisory.			
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Prime Infrastructure and Cisco Evolved Programmable			
		Network Manager (EPNM) could allow a remote attacker to obtain			
		privileged information and conduct cross-site scripting (XSS) and			
	cisco - multiple	cross-site request forgery (CSRF) attacks. For more information			
CVE-2023-20130	products	about these vulnerabilities, see the Details section of this advisory.	2023-04-05	6.5	Medium
		Multiple vulnerabilities in the web interface of Cisco Webex			
		Meetings could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack or upload			
	cisco -	arbitrary files as recordings. For more information about these			
CVE-2023-20134	webex_meetings	vulnerabilities, see the Details section of this advisory.	2023-04-05	6.5	Medium
		The IBM Toolbox for Java (Db2 Mirror for i 7.4 and 7.5) could allow			
		a user to obtain sensitive information, caused by utilizing a Java			
		string for processing. Since Java strings are immutable, their			
		contents exist in memory until garbage collected. This means			
		sensitive data could be visible in memory over an indefinite			
		amount of time. IBM has addressed this issue by reducing the			
0) /5 2022 42020	ibm - multiple	amount of time the sensitive data is visible in memory. IBM X-	2022 24 27	6.5	
CVE-2022-43928	products	Force ID: 241675.	2023-04-07	6.5	Medium
		In vdec, there is a possible use after free due to a race condition.			
	google - multiple	This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for			
CVE-2023-20684	googie - muitipie products	execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069.	2023-04-06	6.4	Medium
<u> </u>	products	In vdec, there is a possible use after free due to a race condition.	2023-04-00	U. 4	ivicululli
		This could lead to local escalation of privilege with System			
	google - multiple	execution privileges needed. User interaction is not needed for			
CVE-2023-20685	products	exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575.	2023-04-06	6.4	Medium
		In display drm, there is a possible double free due to a race			
		condition. This could lead to local escalation of privilege with			
		System execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation. Patch ID: ALPS07570826; Issue ID:			
CVE-2023-20686	products	ALPS07570826.	2023-04-06	6.4	Medium
		In display drm, there is a possible double free due to a race			
		condition. This could lead to local escalation of privilege with			
	google - multiple	System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570772; Issue ID:			
CVE-2023-20687	products	ALPS07570772.	2023-04-06	6.4	Medium
CVL-2023-20087	products	A use-after-free flaw was found in btrfs_search_slot in	2023-04-00	0.4	Mediaiii
		fs/btrfs/ctree.c in btrfs in the Linux Kernel.This flaw allows an			
		attacker to crash the system and possibly cause a kernel			
CVE-2023-1611	linux - linux_kernel	information lea	2023-04-03	6.3	Medium
		A use-after-free flaw was found in xgene_hwmon_remove in			
		drivers/hwmon/xgene-hwmon.c in the Hardware Monitoring Linux			
		Kernel Driver (xgene-hwmon). This flaw could allow a local			
	linux - multiple	attacker to crash the system due to a race problem. This			
CVE-2023-1855	products	vulnerability could even lead to a kernel information leak problem.	2023-04-05	6.3	Medium
		Veritas NetBackUp OpsCenter Version 9.1.0.1 is vulnerable to			
	veritas -	Reflected Cross-site scripting (XSS). The Web App fails to adequately sanitize special characters. By leveraging this issue, an			
	netbackup_opscent	attacker is able to cause arbitrary HTML and JavaScript code to be			
CVE-2023-26789	er	executed in a user's browser.	2023-04-05	6.1	Medium
212 2020 20705	<u> </u>	A vulnerability in the web-based management interface of Cisco		J.1	Gaiaiii
		Prime Infrastructure Software could allow an unauthenticated,			
		remote attacker to conduct a reflected cross-site scripting (XSS)			
		attack against a user of the interface on an affected device. This			
		vulnerability is due to insufficient validation of user-supplied input.			
		An attacker could exploit this vulnerability by persuading a user of			
		the web-based management interface on an affected device to			
	cisco -	click a crafted link. A successful exploit could allow the attacker to			
	prime_infrastructur	execute arbitrary script code in the context of the affected			
CVE-2023-20068	е	interface or to access sensitive, browser-based information.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		, ,			
		requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful			
		requests to an affected device and then persuading a user to visit			
		requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful			
	cisco -	requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in			
CVE-2023-20137	cisco - rv016_firmware	requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20137 CVE-2023-20138		requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that	2023-04-05	6.1	Medium Medium

		Taylor 2		1	I
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
		based information. Cisco has not released software updates that			
		address these vulnerabilities.			
		Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-			
	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20139	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20140	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
	cisco	the context of the affected interface or access sensitive, browser-			
CVE-2023-20141	cisco - rv016_firmware	based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVL 2023 20141	TVOIO_IIIIIWaic	Multiple vulnerabilities in the web-based management interface of	2023 04 03	0.1	Wicalam
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20142	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
	cisco	the context of the affected interface or access sensitive, browser-			
CVE-2023-20143	cisco - rv016 firmware	based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVL-2023-20143	14010_IIIIIIWale	Multiple vulnerabilities in the web-based management interface of	2023-04-03	0.1	ivicululli
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
	cisco -	RV325 Routers could allow an unauthenticated, remote attacker			
CVE-2023-20144	rv016_firmware	to conduct cross-site scripting (XSS) attacks against a user of the	2023-04-05	6.1	Medium

				ı	1
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
		based information. Cisco has not released software updates that			
		address these vulnerabilities.			
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20145	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20146	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
0.45 0000 004 45	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20147	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
	cisco -	the context of the affected interface or access sensitive, browser- based information. Cisco has not released software updates that			
CVE-2023-20148	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
<u> </u>		Multiple vulnerabilities in the web-based management interface of		J.1	caiaiii
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20149	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
	cisco	to conduct cross-site scripting (XSS) attacks against a user of the			
CVE-2023-20150	cisco - rv016_firmware	interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker	2023-04-05	6.1	Medium
CAT-5052-50120	I AOTO III III Male	vanuation by the web-based management interface. All attacker	2023-04-03	0.1	ivicululli

Γ					1
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
		based information. Cisco has not released software updates that			
		address these vulnerabilities.			
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and			
		RV325 Routers could allow an unauthenticated, remote attacker			
		to conduct cross-site scripting (XSS) attacks against a user of the			
		interface. These vulnerabilities are due to insufficient input			
		validation by the web-based management interface. An attacker			
		could exploit these vulnerabilities by sending crafted HTTP			
		requests to an affected device and then persuading a user to visit			
		specific web pages that include malicious payloads. A successful			
		exploit could allow the attacker to execute arbitrary script code in			
		the context of the affected interface or access sensitive, browser-			
	cisco -	based information. Cisco has not released software updates that			
CVE-2023-20151	rv016_firmware	address these vulnerabilities.	2023-04-05	6.1	Medium
		A vulnerability in the web-based management interface of Cisco			
		Identity Services Engine (ISE) could allow an authenticated, remote			
		attacker to access sensitive information, conduct a server-side			
		request forgery (SSRF) attack through an affected device, or			
		negatively impact the responsiveness of the web-based			
		management interface itself. This vulnerability is due to improper			
		handling of XML External Entity (XXE) entries when parsing certain			
		XML files. An attacker could exploit this vulnerability by uploading			
		a crafted XML file that contains references to external entities. A			
		successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of confidential			
		information. A successful exploit could also cause the web			
		application to perform arbitrary HTTP requests on behalf of the			
		attacker or consume memory resources to reduce the availability			
		of the web-based management interface. To successfully exploit			
	cisco - multiple	this vulnerability, an attacker would need valid Super Admin or			
CVE-2023-20030	products	Policy Admin credentials.	2023-04-05	6	Medium
012 2020 20000	products	The Samba AD DC administration tool, when operating against a	2020 0 1 00		Mediam
	samba - multiple	remote LDAP server, will by default send new or reset passwords			
CVE-2023-0922	products	over a signed-only connection.	2023-04-03	5.9	Medium
	Р	IBM WebSphere Application Server 9.0 is vulnerable to cross-site			
		scripting. This vulnerability allows users to embed arbitrary			
	ibm -	JavaScript code in the Web UI thus altering the intended			
	websphere_applica	functionality potentially leading to credentials disclosure within a			
CVE-2023-26283	tion_server	trusted session. IBM X-Force ID: 248416.	2023-04-02	5.4	Medium
		Jenkins JaCoCo Plugin 3.3.2 and earlier does not escape class and			
		method names shown on the UI, resulting in a stored cross-site			
		scripting (XSS) vulnerability exploitable by attackers able to control			
		input files for the 'Record JaCoCo coverage report' post-build			
CVE-2023-28669	jenkins - jacoco	action.	2023-04-02	5.4	Medium
		Jenkins Pipeline Aggregator View Plugin 1.13 and earlier does not			
		escape a variable representing the current view's URL in inline			
	jenkins -	JavaScript, resulting in a stored cross-site scripting (XSS)			
	pipeline_aggregato	vulnerability exploitable by authenticated attackers with			
CVE-2023-28670	r_view	Overall/Read permission.	2023-04-02	5.4	Medium
		Jenkins Cppcheck Plugin 1.26 and earlier does not escape file			
		names from Cppcheck report files before showing them on the			
		Jenkins UI, resulting in a stored cross-site scripting (XSS)			
CVE 2022 20070	ionking appet!	vulnerability exploitable by attackers able to control report file	2022 04 02	E 4	Madi
CVE-2023-28678	jenkins - cppcheck	contents.	2023-04-02	5.4	Medium
		Jenkins Mashup Portlets Plugin 1.1.2 and earlier provides the			
		"Generic JS Portlet" feature that lets a user populate a portlet using a custom JavaScript expression, resulting in a stored cross-			
	jenkins -	site scripting (XSS) vulnerability exploitable by authenticated			
CVE-2023-28679	mashup_portlets	attackers with Overall/Read permission.	2023-04-02	5.4	Medium
CAF 7052-50013	masnap_portiets	A reflected XSS via POST vulnerability in report scheduler of	2023 04-02	J. 4	IVICUIUIII
		Sophos Web Appliance versions older than 4.3.10.4 allows			
		execution of JavaScript code in the victim browser via a malicious			
	sophos -	form that must be manually submitted by the victim while logged			
CVE-2020-36692	web_appliance	in to SWA.	2023-04-04	5.4	Medium
		Dell Streaming Data Platform prior to 1.4 contains Open Redirect			
	dell -	vulnerability. An attacker with privileges same as a legitimate user			
	streaming_data_pl	can phish the legitimate the user to redirect to malicious website			
CVE-2023-28069	atform	leading to information disclosure and launch of phishing attacks.	2023-04-05	5.4	Medium
		Multiple vulnerabilities in the web-based management interface of			
		Cisco Prime Infrastructure and Cisco Evolved Programmable			
	cisco - multiple	Network Manager (EPNM) could allow a remote attacker to obtain			
CVE-2023-20131	products	privileged information and conduct cross-site scripting (XSS) and	2023-04-05	5.4	Medium

		cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack or upload			
CVE-2023-20132	cisco - webex_meetings	arbitrary files as recordings. For more information about these vulnerabilities, see the Details section of this advisory.	2023-04-05	5.4	Medium
CVL-2023-20132	webex_ineetings	A vulnerability in the web-based management interface of Cisco	2023-04-03	5.4	Mediaiii
	cisco - unified_contact_ce	Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack. This vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by entering crafted text into various input fields within the web-based management interface. A successful exploit could allow the attacker to perform a stored XSS attack, which could allow the execution of scripts within the context of other			
CVE-2023-20096	nter express	users of the interface.	2023-04-05	5.4	Medium
	ibm - tririga_application_	IBM TRIRIGA Application Platform 4.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a			
CVE-2022-43914	platform	trusted session. IBM X-Force ID: 241036.	2023-04-07	5.4	Medium
CVE-2023-1582	linux - multiple products	A race problem was found in fs/proc/task_mmu.c in the memory management sub-component in the Linux kernel. This issue may allow a local attacker with user privilege to cause a denial of service. A vulnerability in the offline access mode of Cisco Duo Two-Factor	2023-04-05	4.7	Medium
	cisco - multiple	Authentication for macOS and Duo Authentication for Windows Logon and RDP could allow an unauthenticated, physical attacker to replay valid user session credentials and gain unauthorized access to an affected macOS or Windows device. This vulnerability exists because session credentials do not properly expire. An attacker could exploit this vulnerability by replaying previously used multifactor authentication (MFA) codes to bypass MFA protection. A successful exploit could allow the attacker to gain			
CVE-2023-20123	products	unauthorized access to the affected device.	2023-04-05	4.6	Medium
	google - multiple	In wlan, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID:			
CVE-2023-20660	products	ALPS07588383.	2023-04-06	4.4	Medium
CVE-2023-20665	google - multiple products	In ril, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. In wlan, there is a possible out of bounds read due to a missing bounds about This could lead to local information disclosure with	2023-04-06	4.4	Medium
		bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not			
	google - multiple	needed for exploitation. Patch ID: ALPS07588569; Issue ID:			
CVE-2023-20674	products	ALPS07588552.	2023-04-06	4.4	Medium
	google - multiple	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID:			
CVE-2023-20675	products	ALPS07588569. In wlan, there is a possible out of bounds read due to a missing	2023-04-06	4.4	Medium
	google - multiple	bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID:			
CVE-2023-20676	products	ALPS07628518.	2023-04-06	4.4	Medium
CVE-2023-20677	google - multiple products	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436.	2023-04-06	4.4	Medium
CVE 2022 20070	google - multiple	In wlan, there is a possible out of bounds read 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: ALPSO7588413; Issue ID:	2022 04 06	A A	Madium
CVE-2023-20679	products google - multiple	ALPS07588453. In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID:	2023-04-06	4.4	Medium
		,	1		1
CVE-2023-20688	products	ALPS07441821.	2023-04-06	4.4	Medium
CVE-2023-20688		ALPS07441821. A cross-site request forgery (CSRF) vulnerability in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.0 and earlier allows	2023-04-06	4.4	Medium

		specified credentials IDs obtained through another method,			
		capturing credentials stored in Jenkins.			
		A missing permission check in Jenkins OctoPerf Load Testing Plugin			
	jenkins -	Plugin 4.5.2 and earlier allows attackers with Overall/Read			
	octoperf_load_testi	permission to enumerate credentials IDs of credentials stored in			
CVE-2023-28673	ng	Jenkins.	2023-04-02	4.3	Medium
	jenkins -	A missing permission check in Jenkins OctoPerf Load Testing Plugin			
	octoperf_load_testi	Plugin 4.5.2 and earlier allows attackers to connect to a previously			
CVE-2023-28675	ng	configured Octoperf server using attacker-specified credentials.	2023-04-02	4.3	Medium
		A flaw was found in Samba. An incomplete access check on			
	samba - multiple	dnsHostName allows authenticated but otherwise unprivileged			
CVE-2023-0225	products	users to delete this attribute from any object in the directory.	2023-04-03	4.3	Medium

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.