National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 – 15 Apr 2023 Vol. 10 No. 07

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: ABB					
Product: my_control_system					
Affected Version(s): From (including) 5.0 Up to (including) 5.13					
Insecure Storage of Sensitive Information	06-Apr-2023	9.8	Insecure Storage of Sensitive Information vulnerability in ABB My Control System (on-premise) allows an attacker who successfully exploited this vulnerability to gain access to the secure application data or take control of the application. Of the services that make up the My Control System (on-premise) application, the following ones are affected by this vulnerability: User Interface System Monitoring1 Asset Inventory This issue affects My Control System (on-premise): from 5.0;0 through 5.13. **CVE ID : CVE-2023-0580**	https://search.abb.com/library/Download.aspx?DocumentID=7PAA007893&LanguageCode=en&DocumentPartId=&Action=Launch	A-ABB-MY_C-200423/1
Vendor: Adobe					
Product: dimension					
Affected Version(s): * Up to (including) 3.4.8					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26371**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/2
Out-of-bounds Write	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26372**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26373**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/4
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26374**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/5
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to	https://helpx.adobe.com/security/products/dimension/	A-ADO-DIME-200423/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26375**	apsb23-27.html	
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26376**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/7
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26377**		
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26378**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/9
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26379**		
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26380**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/11
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26381**		
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26382**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/13
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-26400**		
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26401**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/15
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	A-ADO-DIME-200423/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26404		
Product: livecycle_es4					
Affected Version(s): * Up to (excluding) 11.0.1					
Deserialization of Untrusted Data	06-Apr-2023	9.8	** UNSUPPORTED WHEN ASSIGNED ** A Java insecure 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	N/A	A-ADO-LIVE-200423/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account that is running the Adobe LiveCycle application. If the account is privileged, exploitation provides privileged access to the operating system. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2023-28500**		
Vendor: air_cargo_management_system_project					
Product: air_cargo_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	9.8	A vulnerability has been found in SourceCodester Air Cargo Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/transactions/track_shipment.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the	N/A	A-AIR-AIR_-200423/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The associated identifier of this vulnerability is VDB-224995. **CVE ID : CVE-2023-1856**		
Vendor: akbim					
Product: panon					
Affected Version(s): * Up to (excluding) 1.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Apr-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Akbim Computer Panon allows SQL Injection.This issue affects Panon: before 1.0.2. **CVE ID : CVE-2023-1765**	N/A	A-AKB-PANO-200423/19
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Akbim Computer Panon allows Reflected XSS.This issue affects Panon: before 1.0.2. **CVE ID : CVE-2023-1766**	N/A	A-AKB-PANO-200423/20
Vendor: albo_pretorio_on_line_project					
Product: albo_pretorio_on_line					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ignazio Scimone Albo Pretorio On Line plugin <= 4.6.1 versions. **CVE ID : CVE-2023-28993**	N/A	A-ALB-ALBO-200423/21
Vendor: Allegro					
Product: bigflow					
Affected Version(s): * Up to (excluding) 1.6					
Improper Certificate Validation	10-Apr-2023	5.9	Allegro Tech BigFlow <1.6 is vulnerable to Missing SSL Certificate Validation. **CVE ID : CVE-2023-25392**	https://github.com/allegro/bigflow/pull/357	A-ALL-BIGF-200423/22
Vendor: announce_from_the_dashboard_project					
Product: announce_from_the_dashboard					
Affected Version(s): * Up to (including) 1.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth (admin+) Stored Cross-Site Scripting (XSS) vulnerability in gqevu6bsiz Announce from the Dashboard plugin <= 1.5.1 versions. **CVE ID : CVE-2023-25716**	N/A	A-ANN-ANNO-200423/23
Vendor: Apache					
Product: airflow_drill_provider					
Affected Version(s): * Up to (excluding) 2.3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	07-Apr-2023	7.5	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Drill Provider.This issue affects Apache Airflow Drill Provider: before 2.3.2. **CVE ID : CVE-2023-28707**	https://github.com/apache/airflow/pull/30215, https://lists.apache.org/thread/dfoj7q1nd0vhhsl8fjg63z4j6mfmdxtk	A-APA-AIRF-200423/24
Product: airflow_hive_provider					
Affected Version(s): * Up to (excluding) 6.0.0					
Improper Control of Generation of Code ('Code Injection')	07-Apr-2023	9.8	Improper Control of Generation of Code ('Code Injection') vulnerability in Apache Software Foundation Apache Airflow Hive Provider.This issue affects Apache Airflow Hive Provider: before 6.0.0. **CVE ID : CVE-2023-28706**	https://github.com/apache/airflow/pull/30212, https://lists.apache.org/thread/dl20xxd51xvlx0zzc0wzgxfjwgtbbxo3	A-APA-AIRF-200423/25
Product: airflow_spark_provider					
Affected Version(s): * Up to (excluding) 4.0.1					
Improper Input Validation	07-Apr-2023	7.5	Improper Input Validation vulnerability in Apache Software Foundation Apache	https://github.com/apache/airflow/pull/30223, https://lists.a	A-APA-AIRF-200423/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Airflow Spark Provider.This issue affects Apache Airflow Spark Provider: before 4.0.1. **CVE ID : CVE-2023-28710**	pache.org/thread/lb9w9114ow00h2nkn8bjm106v5x1p1d2	
Product: http_server					
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.4.13.2					
NULL Pointer Dereference	03-Apr-2023	7.5	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 contains a patch for this issue. As a workaround, avoid	https://github.com/OpenIDC/mod_auth_openidc/commit/c0e1edac3c4c19988ccdc7713d7aebfce6ff916a	A-APA-HTTP-200423/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using `OIDCStripCookies`. **CVE ID : CVE-2023-28625**		
Product: james					
Affected Version(s): * Up to (excluding) 3.7.4					
Missing Authorization	03-Apr-2023	7.8	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 Guice users. **CVE ID : CVE-2023-26269**	N/A	A-APA-JAME-200423/28
Product: linkis					
Affected Version(s): * Up to (including) 1.3.1					
Unrestricted Upload of File with	10-Apr-2023	9.8		https://lists.apache.org/thread/wt70jfc0	A-APA-LINK-200423/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

Dangerous Type			In Apache Linkis <=1.3.1, The PublicService module uploads files without restrictions on the path to the uploaded files, and file types.
			We recommend users upgrade the version of Linkis to version 1.3.2.
			For versions
			<=1.3.1, we suggest turning on the file path check switch in linkis.properties
			`wds.linkis.workspace.filesystem.owner.check=true`
			`wds.linkis.workspace.filesystem.path.check=true`
			CVE ID : CVE-2023-27602
				yfs6s5g0wg5dr5klnc48nsp1	

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Apr-2023	9.8	In Apache Linkis <=1.3.1, due to the Manager module engineConn material upload does not check the zip	https://lists.apache.org/thread/6n1vlvnyn441rm02zdqc0wnpckj8ltn8	A-APA-LINK-200423/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path, This is a Zip Slip issue, which will lead to a potential RCE vulnerability. We recommend users upgrade the version of Linkis to version 1.3.2. **CVE ID : CVE-2023-27603**		
Deserialization of Untrusted Data	10-Apr-2023	9.8	In Apache Linkis <=1.3.1, due to the lack of effective filtering of parameters, an attacker configuring malicious Mysql JDBC parameters in JDBC EengineConn Module will trigger a deserialization vulnerability and eventually lead to remote code execution. Therefore, the parameters in the Mysql JDBC URL should be blacklisted. Versions of Apache Linkis <= 1.3.0 will be affected. We recommend users upgrade the	https://lists.apache.org/thread/o682wz1ggq491ybvjwokxvcdtnzo76ls	A-APA-LINK-200423/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version of Linkis to version 1.3.2. **CVE ID : CVE-2023-29215**		
Deserialization of Untrusted Data	10-Apr-2023	9.8	In Apache Linkis <=1.3.1, because the parameters are not effectively filtered, the attacker uses the MySQL data source and malicious parameters to configure a new data source to trigger a deserialization vulnerability, eventually leading to remote code execution. Versions of Apache Linkis <= 1.3.0 will be affected. We recommend users upgrade the version of Linkis to version 1.3.2. **CVE ID : CVE-2023-29216**	https://lists.apache.org/thread/18vv0m32oy51nzk8tbz13qdl5569y55l	A-APA-LINK-200423/32
Inadequate Encryption Strength	10-Apr-2023	9.1	In Apache Linkis <=1.3.1, due to the	https://lists.apache.org/thread/3cr1cz3210wzwngldwr	A-APA-LINK-200423/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	default token generated by Linkis Gateway deployment being too simple, it is easy for attackers to obtain the default token for the attack. Generation rules should add random values. We recommend users upgrade the version of Linkis to version 1.3.2 And modify the default token value. You can refer to Token authorization[1] https://linkis.apache.org/docs/latest/auth/token https://linkis.apache.org/docs/latest/auth/token **CVE ID : CVE-2023-27987**	qzm43vwhghp0p	
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 16.4.1					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Apr-2023	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28205**	N/A	A-APP-SAFA-200423/34
Vendor: apusapps					
Product: launcher					
Affected Version(s): 3.10.73					
N/A	10-Apr-2023	9.8	An issue found in APUS Group Launcher v.3.10.73 and v.3.10.88 allows a remote attacker to execute arbitrary code via the FONT_FILE parameter. **CVE ID : CVE-2023-27650**	N/A	A-APU-LAUN-200423/35
Affected Version(s): 3.10.88					
N/A	10-Apr-2023	9.8	An issue found in APUS Group Launcher v.3.10.73 and v.3.10.88 allows a remote attacker to	N/A	A-APU-LAUN-200423/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code via the FONT_FILE parameter. **CVE ID : CVE-2023-27650**		
Vendor: ARM					
Product: avalon_gpu_kernel_driver					
Affected Version(s): From (including) r41p0 Up to (excluding) r43p0					
Missing Release of Memory after Effective Lifetime	06-Apr-2023	5.5	Memory leak vulnerability in Mali GPU Kernel Driver in Midgard GPU Kernel Driver all versions from r6p0 - r32p0, Bifrost GPU Kernel Driver all versions from r0p0 - r42p0, Valhall GPU Kernel Driver all versions from r19p0 - r42p0, and Avalon GPU Kernel Driver all versions from r41p0 - r42p0 allows a non-privileged user to make valid GPU processing operations that expose sensitive kernel metadata. **CVE ID : CVE-2023-26083**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-AVAL-200423/37
Product: bifrost_gpu_kernel_driver					
Affected Version(s): From (including) r0p0 Up to (excluding) r43p0					
Missing Release of Memory after Effective Lifetime	06-Apr-2023	5.5	Memory leak vulnerability in Mali GPU Kernel Driver in Midgard GPU Kernel Driver all versions from r6p0 - r32p0,	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver	A-ARM-BIFR-200423/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bifrost GPU Kernel Driver all versions from r0p0 - r42p0, Valhall GPU Kernel Driver all versions from r19p0 - r42p0, and Avalon GPU Kernel Driver all versions from r41p0 - r42p0 allows a non-privileged user to make valid GPU processing operations that expose sensitive kernel metadata. **CVE ID : CVE-2023-26083**	%20Vulnerabilities	
Product: midgard					
Affected Version(s): From (including) r6p0 Up to (including) r32p0					
Missing Release of Memory after Effective Lifetime	06-Apr-2023	5.5	Memory leak vulnerability in Mali GPU Kernel Driver in Midgard GPU Kernel Driver all versions from r6p0 - r32p0, Bifrost GPU Kernel Driver all versions from r0p0 - r42p0, Valhall GPU Kernel Driver all versions from r19p0 - r42p0, and Avalon GPU Kernel Driver all versions from r41p0 - r42p0 allows a non-privileged user to make valid GPU processing operations that expose sensitive kernel metadata.	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-MIDG-200423/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26083		
Product: valhall_gpu_kernel_driver					
Affected Version(s): From (including) r19p0 Up to (excluding) r43p0					
Missing Release of Memory after Effective Lifetime	06-Apr-2023	5.5	Memory leak vulnerability in Mali GPU Kernel Driver in Midgard GPU Kernel Driver all versions from r6p0 - r32p0, Bifrost GPU Kernel Driver all versions from r0p0 - r42p0, Valhall GPU Kernel Driver all versions from r19p0 - r42p0, and Avalon GPU Kernel Driver all versions from r41p0 - r42p0 allows a non-privileged user to make valid GPU processing operations that expose sensitive kernel metadata. **CVE ID : CVE-2023-26083**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-VALH-200423/40
Vendor: article_directory_project					
Product: article_directory					
Affected Version(s): * Up to (including) 1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The Article Directory WordPress plugin through 1.3 does not properly sanitize the `publish_terms_text` setting before displaying it in the administration panel, which may enable	N/A	A-ART-ARTI-200423/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrators to conduct Stored XSS attacks in multisite contexts. **CVE ID : CVE-2023-0422**		
Vendor: atlauncher					
Product: atlauncher					
Affected Version(s): * Up to (excluding) 3.4.27.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Apr-2023	7.1	ATLauncher <= 3.4.26.0 is vulnerable to Directory Traversal. A mrpack file can be maliciously crafted to create arbitrary files outside of the installation directory. **CVE ID : CVE-2023-25303**	https://github.com/ATLauncher/ATLauncher/security/advisories/GHSA-7cff-8xv4-mvx6	A-ATL-ATLA-200423/42
Vendor: atos					
Product: unify_openscape_4000					
Affected Version(s): 10					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-2023	9.8	webservice in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23710.	https://networks.unify.com/security/advisories/OBSO-2303-01.pdf	A-ATO-UNIF-200423/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29473		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-2023	9.8	inventory in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23552. **CVE ID : CVE-2023-29474**	https://networks.unify.com/security/advisories/OBSO-2303-01.pdf	A-ATO-UNIF-200423/44
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-2023	9.8	inventory in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23543. **CVE ID : CVE-2023-29475**	https://networks.unify.com/security/advisories/OBSO-2303-01.pdf	A-ATO-UNIF-200423/45
Product: unify_openscape_4000_manager					
Affected Version(s): 10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-2023	9.8	webservice in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23710. **CVE ID : CVE-2023-29473**	https://networks.unify.com/security/advisories/OBSO-2303-01.pdf	A-ATO-UNIF-200423/46
Improper Neutralization of Special Elements used in a Command ('Command Injection')	06-Apr-2023	9.8	inventory in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23552. **CVE ID : CVE-2023-29474**	https://networks.unify.com/security/advisories/OBSO-2303-01.pdf	A-ATO-UNIF-200423/47
Improper Neutralization of Special Elements used in a Command	06-Apr-2023	9.8	inventory in Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform 10 R1 before 10 R1.34.4 allows an	https://networks.unify.com/security/advisories/OBSO-2303-01.pdf	A-ATO-UNIF-200423/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			unauthenticated attacker to run arbitrary commands on the platform operating system and achieve administrative access, aka OSFOURK-23543. **CVE ID : CVE-2023-29475**		
Vendor: auto_hide_admin_bar_project					
Product: auto_hide_admin_bar					
Affected Version(s): * Up to (including) 1.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marcel Bootsman Auto Hide Admin Bar plugin <= 1.6.1 versions. **CVE ID : CVE-2023-23994**	N/A	A-AUT-AUTO-200423/49
Vendor: auto_rename_media_on_upload_project					
Product: auto_rename_media_on_upload					
Affected Version(s): * Up to (excluding) 1.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The Auto Rename Media On Upload WordPress plugin before 1.1.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is	N/A	A-AUT-AUTO-200423/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disallowed (for example in multisite setup). **CVE ID : CVE-2023-0605**		
Vendor: avalex					
Product: avalex					
Affected Version(s): * Up to (including) 3.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in avalex GmbH avalex – Automatically secure legal texts plugin <= 3.0.3 versions. **CVE ID : CVE-2023-25059**	N/A	A-AVA-AVAL-200423/51
Vendor: bank_locker_management_system_project					
Product: bank_locker_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Apr-2023	9.8	A vulnerability was found in PHPGurukul Bank Locker Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php of the component Search. The manipulation of the argument searchinput leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the	N/A	A-BAN-BANK-200423/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The associated identifier of this vulnerability is VDB-225359. **CVE ID : CVE-2023-1963**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Apr-2023	9.1	A vulnerability classified as critical has been found in PHPGurukul Bank Locker Management System 1.0. Affected is an unknown function of the file recovery.php of the component Password Reset. The manipulation of the argument uname/mobile leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225360. **CVE ID : CVE-2023-1964**	N/A	A-BAN-BANK-200423/53
Vendor: Bestwebsoft					
Product: user_role					
Affected Version(s): * Up to (excluding) 1.6.7					
Cross-Site Request Forgery (CSRF)	03-Apr-2023	8.8	The User Role by BestWebSoft WordPress plugin before 1.6.7 does not protect against CSRF in requests to update role capabilities,	N/A	A-BES-USER-200423/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to arbitrary privilege escalation of any role. **CVE ID : CVE-2023-0820**		
Vendor: best_online_news_portal_project					
Product: best_online_news_portal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Apr-2023	9.8	A vulnerability classified as critical was found in SourceCodester Best Online News Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225361 was assigned to this vulnerability. **CVE ID : CVE-2023-1962**	N/A	A-BES-BEST-200423/55
Vendor: bibliocraftmod					
Product: bibliocraft					
Affected Version(s): * Up to (excluding) 2.4.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Apr-2023	9.8	BiblioCraft before 2.4.6 does not sanitize path-traversal characters in filenames, allowing restricted write access to almost anywhere on the filesystem. This includes the Minecraft mods folder, which results in code execution. **CVE ID : CVE-2023-29478**	N/A	A-BIB-BIBL-200423/56
Vendor: bigfork					
Product: silverstripe_form_capture					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Silverstripe Form Capture provides a method to capture simple silverstripe forms and an admin interface for users. Starting in version 0.2.0 and prior to versions 1.0.2, 1.1.0, 2.2.5, and 3.1.1, improper escaping when presenting stored form submissions allowed for an attacker to perform a Cross-Site Scripting attack. The vulnerability was initially patched in version 1.0.2, and version 1.1.0 includes this patch. The bug was then accidentally re-	https://github.com/bigfork/silverstripe-form-capture/security/advisories/GHSA-38h6-gmr2-j4wx, https://github.com/bigfork/silverstripe-form-capture/commit/5b3aa39dd1eef042f173167b0fa4d3f717971772	A-BIG-SILV-200423/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			introduced during a merge error, and has been re-patched in versions 2.2.5 and 3.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28851**		
Affected Version(s): 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Silverstripe Form Capture provides a method to capture simple silverstripe forms and an admin interface for users. Starting in version 0.2.0 and prior to versions 1.0.2, 1.1.0, 2.2.5, and 3.1.1, improper escaping when presenting stored form submissions allowed for an attacker to perform a Cross-Site Scripting attack. The vulnerability was initially patched in version 1.0.2, and version 1.1.0 includes this patch. The bug was then accidentally re-introduced during a merge error, and has been re-patched in versions 2.2.5 and 3.1.1. There are no known workarounds for this vulnerability.	https://github.com/bigfork/silverstripe-form-capture/security/advisories/GHSA-38h6-gmr2-j4wx, https://github.com/bigfork/silverstripe-form-capture/commit/5b3aa39dd1eef042f173167b0fa4d3f717971772	A-BIG-SILV-200423/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28851		
Affected Version(s): 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Silverstripe Form Capture provides a method to capture simple silverstripe forms and an admin interface for users. Starting in version 0.2.0 and prior to versions 1.0.2, 1.1.0, 2.2.5, and 3.1.1, improper escaping when presenting stored form submissions allowed for an attacker to perform a Cross-Site Scripting attack. The vulnerability was initially patched in version 1.0.2, and version 1.1.0 includes this patch. The bug was then accidentally re-introduced during a merge error, and has been re-patched in versions 2.2.5 and 3.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28851**	https://github.com/bigfork/silverstripe-form-capture/security/advisories/GHSA-38h6-gmr2-j4wx, https://github.com/bigfork/silverstripe-form-capture/commit/5b3aa39dd1eef042f173167b0fa4d3f717971772	A-BIG-SILV-200423/59
Affected Version(s): 3.1.0					
Improper Neutralization of Input During	03-Apr-2023	5.4	Silverstripe Form Capture provides a method to capture simple silverstripe forms and an admin	https://github.com/bigfork/silverstripe-form-capture/secur	A-BIG-SILV-200423/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			interface for users. Starting in version 0.2.0 and prior to versions 1.0.2, 1.1.0, 2.2.5, and 3.1.1, improper escaping when presenting stored form submissions allowed for an attacker to perform a Cross-Site Scripting attack. The vulnerability was initially patched in version 1.0.2, and version 1.1.0 includes this patch. The bug was then accidentally re-introduced during a merge error, and has been re-patched in versions 2.2.5 and 3.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28851**	ity/advisories/GHSA-38h6-gmr2-j4wx, https://github.com/bigfork/silverstripe-form-capture/commit/5b3aa39dd1eef042f173167b0fa4d3f717971772	
Affected Version(s): From (including) 0.2.0 Up to (including) 0.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Silverstripe Form Capture provides a method to capture simple silverstripe forms and an admin interface for users. Starting in version 0.2.0 and prior to versions 1.0.2, 1.1.0, 2.2.5, and 3.1.1, improper escaping when presenting stored form submissions allowed	https://github.com/bigfork/silverstripe-form-capture/security/advisories/GHSA-38h6-gmr2-j4wx, https://github.com/bigfork/silverstripe-form-capture/commit/5b3aa39d	A-BIG-SILV-200423/61

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for an attacker to perform a Cross-Site Scripting attack. The vulnerability was initially patched in version 1.0.2, and version 1.1.0 includes this patch. The bug was then accidentally re-introduced during a merge error, and has been re-patched in versions 2.2.5 and 3.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28851**	d1eef042f173167b0fa4d3f717971772	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Silverstripe Form Capture provides a method to capture simple silverstripe forms and an admin interface for users. Starting in version 0.2.0 and prior to versions 1.0.2, 1.1.0, 2.2.5, and 3.1.1, improper escaping when presenting stored form submissions allowed for an attacker to perform a Cross-Site Scripting attack. The vulnerability was initially patched in version 1.0.2, and version 1.1.0 includes this patch. The bug was then	https://github.com/bigfork/silverstripe-form-capture/security/advisories/GHSA-38h6-gmr2-j4wx, https://github.com/bigfork/silverstripe-form-capture/commit/5b3aa39dd1eef042f173167b0fa4d3f717971772	A-BIG-SILV-200423/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accidentally re-introduced during a merge error, and has been re-patched in versions 2.2.5 and 3.1.1. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-28851**		
Vendor: bnecreative					
Product: bne_testimonials					
Affected Version(s): * Up to (excluding) 2.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Kerry Kline BNE Testimonials plugin <= 2.0.7 versions. **CVE ID : CVE-2023-24411**	N/A	A-BNE-BNE_-200423/63
Vendor: bp_monitoring_management_system_project					
Product: bp_monitoring_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	9.8	A vulnerability, which was classified as critical, was found in PHPGurukul BP Monitoring Management System 1.0. Affected is an unknown function of the file change-password.php of the component Change Password Handler. The manipulation of the argument password leads to sql injection. It is	N/A	A-BP_-BP_M-200423/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225336. **CVE ID : CVE-2023-1949**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	9.8	A vulnerability has been found in PHPGurukul BP Monitoring Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file password-recovery.php of the component Password Recovery. The manipulation of the argument emailid/contactno leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225337 was assigned to this vulnerability. **CVE ID : CVE-2023-1950**	N/A	A-BP_-BP_M-200423/65
Improper Neutralization of Special	07-Apr-2023	6.5	A vulnerability, which was classified as critical, was found in PHPGurukul BP	N/A	A-BP_-BP_M-200423/66

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Monitoring Management System 1.0. Affected is an unknown function of the file profile.php of the component User Profile Update Handler. The manipulation of the argument name/mobno leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225318 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1909**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Apr-2023	6.1	A vulnerability, which was classified as problematic, has been found in PHPGurukul BP Monitoring Management System 1.0. This issue affects some unknown processing of the file add-family-member.php of the component Add New Family Member Handler. The manipulation of the argument Member Name leads to cross site scripting. The attack may be	N/A	A-BP_-BP_M-200423/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225335. **CVE ID : CVE-2023-1948**		
Vendor: budibase					
Product: budibase					
Affected Version(s): * Up to (excluding) 2.4.3					
Server-Side Request Forgery (SSRF)	06-Apr-2023	6.5	Budibase is a low code platform for creating internal tools, workflows, and admin panels. Versions prior to 2.4.3 (07 March 2023) are vulnerable to Server-Side Request Forgery. This can lead to an attacker gaining access to a Budibase AWS secret key. Users of Budibase cloud need to take no action. Self-host users who run Budibase on the public internet and are using a cloud provider that allows HTTP access to metadata information should ensure that when they deploy Budibase live, their internal metadata	https://github.com/Budibase/budibase/commits/develop?after=93d6939466aec192043d8ac842e754f65fdf2e8a+594&branch=develop&qualified_name=refs%2Fheads%2Fdevelop, https://github.com/Budibase/budibase/security/advisories/GHSA-9xg2-9mcv-985p	A-BUD-BUDI-200423/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			endpoint is not exposed. **CVE ID : CVE-2023-29010**		
Vendor: bzip3_project					
Product: bzip3					
Affected Version(s): * Up to (excluding) 1.2.3					
Out-of-bounds Write	06-Apr-2023	8.8	An issue was discovered in libbzip3.a in bzip3 before 1.2.3. There is an out-of-bounds write in bz3_decode_block. **CVE ID : CVE-2023-29421**	https://github.com/kspalaiologos/bzip3/issues/94	A-BZI-BZIP-200423/69
Out-of-bounds Read	06-Apr-2023	6.5	An issue was discovered in libbzip3.a in bzip3 before 1.2.3. There is an xwrite out-of-bounds read. **CVE ID : CVE-2023-29418**	https://github.com/kspalaiologos/bzip3/commit/aae16d107f804f69000c09cd92027a140968cc9d, https://github.com/kspalaiologos/bzip3/issues/92	A-BZI-BZIP-200423/70
Out-of-bounds Read	06-Apr-2023	6.5	An issue was discovered in libbzip3.a in bzip3 before 1.2.3. There is a bz3_decode_block out-of-bounds read. **CVE ID : CVE-2023-29419**	https://github.com/kspalaiologos/bzip3/issues/92, https://github.com/kspalaiologos/bzip3/commit/8ec8ce7d3d58bf42dabc47e4cc53aa27051bd602	A-BZI-BZIP-200423/71
Improper Restriction	06-Apr-2023	6.5	An issue was discovered in	https://github.com/kspalaio	A-BZI-BZIP-200423/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			libbzip3.a in bzip3 before 1.2.3. There is a crash caused by an invalid memmove in bz3_decode_block. **CVE ID : CVE-2023-29420**	logos/bzip3/commit/bb06deb85f1c249838eb938e0dab271d4194f8fa , https://github.com/kspalaiologos/bzip3/issues/92	
Affected Version(s): * Up to (excluding) 1.3.0					
N/A	06-Apr-2023	6.5	An issue was discovered in libbzip3.a in bzip3 before 1.3.0. A denial of service (process hang) can occur with a crafted archive because bzip3 does not follow the required procedure for interacting with libsais. **CVE ID : CVE-2023-29415**	https://github.com/kspalaiologos/bzip3/issues/95, https://github.com/kspalaiologos/bzip3/compare/1.2.3...1.3.0	A-BZI-BZIP-200423/73
Out-of-bounds Write	06-Apr-2023	6.5	An issue was discovered in libbzip3.a in bzip3 before 1.3.0. A bz3_decode_block out-of-bounds write can occur with a crafted archive because bzip3 does not follow the required procedure for interacting with libsais. **CVE ID : CVE-2023-29416**	https://github.com/kspalaiologos/bzip3/issues/92, https://github.com/kspalaiologos/bzip3/commit/bfa5bf82b53715dfedf048e5859a46cf248668ff	A-BZI-BZIP-200423/74
Affected Version(s): 1.2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	6.5	** DISPUTED ** An issue was discovered in libbzip3.a in bzip3 1.2.2. There is a bz3_decompress out-of-bounds read in certain situations where buffers passed to bzip3 do not contain enough space to be filled with decompressed data. NOTE: the vendor's perspective is that the observed behavior can only occur for a contract violation, and thus the report is invalid. **CVE ID : CVE-2023-29417**	https://github.com/kspalaiologos/bzip3/issues/97	A-BZI-BZIP-200423/75
Vendor: cdesigner_project					
Product: cdesigner					
Affected Version(s): From (including) 3.1.3 Up to (excluding) 3.2.2					
Unrestricted Upload of File with Dangerous Type	07-Apr-2023	9.8	Prestashop cdesigner v3.1.3 to v3.1.8 was discovered to contain a code injection vulnerability via the component CdesignerSaverotateModuleFrontController::initContent(). **CVE ID : CVE-2023-27033**	https://friends-of-presta.github.io/security-advisories/modules/2023/04/06/cdesigner-CWE434.html	A-CDE-CDES-200423/76
Vendor: centralized_covid_vaccination_records_system_project					
Product: centralized_covid_vaccination_records_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Apr-2023	9.8	A vulnerability has been found in SourceCodester Centralized Covid Vaccination Records System 1.0 and classified as critical. This vulnerability affects unknown code of the file /vaccinated/admin/maintenance/manage_location.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-224842 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1827**	N/A	A-CEN-CENT-200423/77
Vendor: cesnet					
Product: libyang					
Affected Version(s): From (including) 2.0.164 Up to (including) 2.1.30					
NULL Pointer Dereference	03-Apr-2023	7.5	libyang from v2.0.164 to v2.1.30 was discovered to contain a NULL pointer dereference via the function lys_parse_mem at lys_parse_mem.c. **CVE ID : CVE-2023-26916**	N/A	A-CES-LIBY-200423/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: chinamobileltd					
Product: oa_mailbox_pc					
Affected Version(s): 2.9.23					
N/A	10-Apr-2023	7.8	An issue in China Mobile OA Mailbox PC v2.9.23 allows remote attackers to execute arbitrary commands on a victim host via user interaction with a crafted EML file sent to their OA mailbox. **CVE ID : CVE-2023-26986**	N/A	A-CHI-OA_M-200423/79
Vendor: churchcrm					
Product: churchcrm					
Affected Version(s): 4.5.3					
Use of Insufficiently Random Values	04-Apr-2023	7.5	The hashing algorithm of ChurchCRM v4.5.3 utilizes a non-random salt value which allows attackers to use precomputed hash tables or dictionary attacks to crack the hashed passwords. **CVE ID : CVE-2023-26855**	N/A	A-CHU-CHUR-200423/80
Vendor: cimatti					
Product: wordpress_contact_forms					
Affected Version(s): * Up to (excluding) 1.5.5					
Improper Neutralization of Input During	07-Apr-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Cimatti Consulting WordPress Contact	N/A	A-CIM-WORD-200423/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Forms by Cimatti plugin <= 1.5.4 versions. **CVE ID : CVE-2023-28781**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Cimatti Consulting WordPress Contact Forms by Cimatti plugin <= 1.5.4 versions. **CVE ID : CVE-2023-28789**	N/A	A-CIM-WORD-200423/82
Vendor: Cisco					
Product: duo					
Affected Version(s): * Up to (excluding) 2.0.1					
Authentication Bypass by Capture-replay	05-Apr-2023	4.6	A vulnerability in the offline access mode of Cisco Duo Two-Factor 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-replay-knuNKd	A-CIS-DUO-200423/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			replaying previously used multifactor authentication (MFA) codes to bypass MFA protection. A successful exploit could allow the attacker to gain unauthorized access to the affected device. **CVE ID : CVE-2023-20123**		
Product: duo_authentication_for_windows_logon_and_rdp					
Affected Version(s): * Up to (excluding) 4.2.2					
Authentication Bypass by Capture-replay	05-Apr-2023	4.6	A vulnerability in the offline access mode of Cisco Duo Two-Factor 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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-replay-knuNKd	A-CIS-DUO_-200423/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(MFA) codes to bypass MFA protection. A successful exploit could allow the attacker to gain unauthorized access to the affected device. **CVE ID : CVE-2023-20123**		
Product: evolved_programmable_network_manager					
Affected Version(s): * Up to (excluding) 5.0.2.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20129**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/85
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	A-CIS-EVOL-200423/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2023-20131**		
Affected Version(s): * Up to (excluding) 7.0.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	6.7	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 gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20121**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk	A-CIS-EVOL-200423/88
Affected Version(s): From (including) 5.1 Up to (excluding) 5.1.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a remote attacker to obtain 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. **CVE ID : CVE-2023-20129**		
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/90
Improper Neutralization of	05-Apr-2023	5.4	Multiple vulnerabilities in the web-based	https://sec.cloudapps.cisco.com/security/c	A-CIS-EVOL-200423/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20131**	enter/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	
Affected Version(s): From (including) 6.0 Up to (excluding) 6.0.2.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2023-20129**		
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/93
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20131**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20129**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/95
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	A-CIS-EVOL-200423/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-EVOL-200423/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2023-20131**		
Product: identity_services_engine					
Affected Version(s): * Up to (excluding) 3.2					
Improper Restriction of XML External Entity Reference	05-Apr-2023	6	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-GecEHY58	A-CIS-IDEN-200423/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 this vulnerability, an attacker would need valid Super Admin or Policy Admin credentials. **CVE ID : CVE-2023-20030**		
Affected Version(s): 3.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	7.8	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 gain root privileges on the underlying operating	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk	A-CIS-IDEN-200423/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20122**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	6.7	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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-os-injection-pxhKsDM	A-CIS-IDEN-200423/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20021		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	6.7	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. **CVE ID : CVE-2023-20022**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-os-injection-pxhKsDM	A-CIS-IDEN-200423/101
Improper Neutralization of Special Elements	05-Apr-2023	6.7	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	A-CIS-IDEN-200423/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			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. **CVE ID : CVE-2023-20023**	Advisory/cisco-sa-ise-os-injection-pxhKsDM	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	6.7	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk	A-CIS-IDEN-200423/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated, local attacker to escape the restricted shell and gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20121**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	6.7	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-2XbOg9Dg	A-CIS-IDEN-200423/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CLI command. A successful exploit could allow the attacker to elevate privileges to root. **CVE ID : CVE-2023-20152**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	6.7	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. **CVE ID : CVE-2023-20153**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-2XbOg9Dg	A-CIS-IDEN-200423/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	05-Apr-2023	6	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-GecEHY58	A-CIS-IDEN-200423/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 this vulnerability, an attacker would need valid Super Admin or Policy Admin credentials. **CVE ID : CVE-2023-20030**		
Product: packet_data_network_gateway					
Affected Version(s): * Up to (excluding) 21.28.0					
N/A	05-Apr-2023	7.5	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 vulnerability by sending a malformed Encapsulating Security Payload (ESP) packet over an IPsec connection. A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pdng-dos-KmzwEy2Q	A-CIS-PACK-200423/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to stop ICMP traffic over an IPsec connection and cause a denial of service (DoS). **CVE ID : CVE-2023-20051**		
Product: prime_infrastructure					
Affected Version(s): * Up to (excluding) 3.10.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	A vulnerability in the web-based management interface of Cisco 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 click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-xss-PU6dnfD9	A-CIS-PRIM-200423/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected interface or to access sensitive, browser-based information. **CVE ID : CVE-2023-20068**		
Affected Version(s): * Up to (excluding) 3.10.4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	6.7	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 gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20121**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-adeos-MLAyEcvk	A-CIS-PRIM-200423/109
Affected Version(s): * Up to (including) 3.7					
N/A	05-Apr-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Network Manager (EPNM) could allow a remote attacker to obtain 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. **CVE ID : CVE-2023-20127**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20129**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/112
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 cross-site request forgery (CSRF) attacks. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20131**		
Affected Version(s): 3.8					
N/A	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20127**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/114
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EPNM) could allow a remote attacker to obtain 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. **CVE ID : CVE-2023-20129**		
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20131**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/117
Affected Version(s): 3.8.1					
N/A	05-Apr-2023	6.5	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 cross-site request forgery (CSRF)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20127**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20129**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/119
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a remote attacker to obtain 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. **CVE ID : CVE-2023-20130**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20131**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/121
Affected Version(s): 3.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20127**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/122
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20129**		
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/124
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain 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. **CVE ID : CVE-2023-20131**		
Affected Version(s): 3.9.1					
N/A	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20127**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/126
Improper Limitation	05-Apr-2023	6.5	Multiple vulnerabilities in the	https://sec.cloudapps.cisco.c	A-CIS-PRIM-200423/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20129**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	
Cross-Site Request Forgery (CSRF)	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2023-20130**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20131**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/129
Affected Version(s): From (including) 3.10 Up to (excluding) 3.10.2					
N/A	05-Apr-2023	6.5	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain 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. **CVE ID : CVE-2023-20127**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Apr-2023	6.5	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20129**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/131
Cross-Site Request	05-Apr-2023	6.5	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	A-CIS-PRIM-200423/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20130**	/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-eRPWAXLe	A-CIS-PRIM-200423/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2023-20131**		
Product: secure_network_analytics					
Affected Version(s): * Up to (excluding) 7.4.2					
Improper Input Validation	05-Apr-2023	7.2	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 code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device. **CVE ID : CVE-2023-20103**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-BDwXFK9C	A-CIS-SECU-200423/134
Affected Version(s): * Up to (including) 7.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	05-Apr-2023	8.8	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 to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the administrator user. **CVE ID : CVE-2023-20102**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealthsmc-rce-sfNBPjcS	A-CIS-SECU-200423/135
Product: unified_contact_center_express					
Affected Version(s): * Up to (excluding) 12.5\\(1\\)su3					
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	5.4	A vulnerability in the web-based management interface of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-xss-GO9L9xxr	A-CIS-UNIF-200423/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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 users of the interface. **CVE ID : CVE-2023-20096**		
Product: webex_meetings					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	6.5	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 arbitrary files as recordings. For	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-sxss-fupl-64uHbcm5	A-CIS-WEBE-200423/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20134**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	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 arbitrary files as recordings. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20132**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-sxss-fupl-64uHbcm5	A-CIS-WEBE-200423/138
Vendor: cloudflare					
Product: warp					
Affected Version(s): * Up to (excluding) 2023.3.381.0					
Improper Link Resolution Before File Access ('Link Following')	06-Apr-2023	7.8	Due to a hardlink created in the ProgramData folder during the repair process of the software, the installer (MSI) of WARP Client for Windows (<= 2022.12.582.0) allowed a malicious attacker to forge the destination of the	https://github.com/cloudflare/advisories/security/advisories/GHSA-xmhj-9p83-xvw9	A-CLO-WARP-200423/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardlink and escalate privileges, overwriting SYSTEM protected files. As Cloudflare WARP client for Windows (up to version 2022.5.309.0) allowed creation of mount points from its ProgramData folder, during installation of the WARP client, it was possible to escalate privileges and overwrite SYSTEM protected files. **CVE ID : CVE-2023-0652**		
Improper Link Resolution Before File Access ('Link Following')	05-Apr-2023	7.8	An unprivileged (non-admin) user can exploit an Improper Access Control vulnerability in the Cloudflare WARP Client for Windows (<= 2022.12.582.0) to perform privileged operations with SYSTEM context by working with a combination of opportunistic locks (oplock) and symbolic links (which can both be created by an unprivileged user). After installing the Cloudflare WARP Client (admin	https://github.com/cloudflare/advisories/security/advisories/GHSA-hgxh-48m3-3gq7	A-CLO-WARP-200423/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges required), an MSI-Installer is placed under C:\Windows\Installer. The vulnerability lies in the repair function of this MSI. ImpactAn unprivileged (non-admin) user can exploit this vulnerability to perform privileged operations with SYSTEM context, including deleting arbitrary files and reading arbitrary file content. This can lead to a variety of attacks, including the manipulation of system files and privilege escalation. PatchesA new installer with a fix that addresses this vulnerability was released in version 2023.3.381.0. While the WARP Client itself is not vulnerable (only the installer), users are encouraged to upgrade to the latest version and delete any older installers present in their systems. **CVE ID : CVE-2023-1412**		
Vendor: codeat					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: glossary					
Affected Version(s): * Up to (excluding) 2.1.28					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Codeat Glossary plugin <= 2.1.27 versions. **CVE ID : CVE-2023-24378**	N/A	A-COD-GLOS-200423/141
Vendor: Codepeople					
Product: wp_time_slots_booking_form					
Affected Version(s): * Up to (including) 1.1.81					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in CodePeople WP Time Slots Booking Form plugin <= 1.1.81 versions. **CVE ID : CVE-2023-23971**	N/A	A-COD-WP_T-200423/142
Vendor: configobj_project					
Product: configobj					
Affected Version(s): *					
N/A	03-Apr-2023	5.9	All versions of the package configobj are vulnerable to Regular Expression Denial of Service (ReDoS) via the validate function, using (.+?)\((.*)\). **Note:** This is only exploitable in the case of a developer, putting the offending	N/A	A-CON-CONF-200423/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value in a server side configuration file. **CVE ID : CVE-2023-26112**		
Vendor: coredial					
Product: sipxcom					
Affected Version(s): * Up to (including) 21.04					
Incorrect Default Permissions	04-Apr-2023	8.8	CoreDial sipXcom up to and including 21.04 is vulnerable to Insecure Permissions. A user who has the ability to run commands as the `daemon` user on a sipXcom server can overwrite a service file, and escalate their privileges to `root`. **CVE ID : CVE-2023-25355**	N/A	A-COR-SIPX-200423/144
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	04-Apr-2023	8.8	CoreDial sipXcom up to and including 21.04 is vulnerable to Improper Neutralization of Argument Delimiters in a Command. XMPP users are able to inject arbitrary arguments into a system command, which can be used to read files from, and write files to, the sipXcom server. This can also be leveraged to gain remote command execution.	N/A	A-COR-SIPX-200423/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25356		
Vendor: creativethemes					
Product: blocksy_companion					
Affected Version(s): * Up to (excluding) 1.8.68					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in CreativeThemes Blocksy Companion plugin <= 1.8.67 versions. **CVE ID : CVE-2023-23898**	N/A	A-CRE-BLOC-200423/146
Vendor: crocoblock					
Product: jetengine_for_elementor					
Affected Version(s): * Up to (excluding) 3.1.3.1					
Unrestricted Upload of File with Dangerous Type	10-Apr-2023	8.8	The JetEngine WordPress plugin before 3.1.3.1 includes uploaded files without adequately ensuring that they are not executable, leading to a remote code execution vulnerability. **CVE ID : CVE-2023-1406**	N/A	A-CRO-JETE-200423/147
Vendor: cththemes					
Product: monolit					
Affected Version(s): * Up to (including) 2.0.6					
Improper Neutralization of Input During	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Cththemes Monolit	N/A	A-CTH-MONO-200423/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			theme <= 2.0.6 versions. **CVE ID : CVE-2023-25041**		
Product: outdoor					
Affected Version(s): * Up to (excluding) 3.9.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Caththemes Outdoor theme <= 3.9.6 versions. **CVE ID : CVE-2023-29236**	N/A	A-CTH-OUTD-200423/149
Vendor: dcac					
Product: time_sheets					
Affected Version(s): * Up to (excluding) 1.29.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The Time Sheets WordPress plugin before 1.29.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-0893**	N/A	A-DCA-TIME-200423/150
Vendor: Dell					
Product: display_manager					
Affected Version(s): * Up to (including) 2.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Least Privilege Violation	06-Apr-2023	7.1	Dell Display Manager, versions 2.1.0 and prior, contains an arbitrary file or folder deletion vulnerability during uninstallation A local low privilege attacker could potentially exploit this vulnerability, leading to the deletion of arbitrary files on the operating system with high privileges. **CVE ID : CVE-2023-28046**	https://www.dell.com/support/kbdoc/en-us/000211727/dsa-2023	A-DEL-DISP-200423/151
Product: power_manager					
Affected Version(s): * Up to (excluding) 3.11					
N/A	07-Apr-2023	7.8	Dell Power Manager, versions 3.10 and prior, contains an Improper Access Control vulnerability. A low-privileged attacker could potentially exploit this vulnerability to elevate privileges on the system. **CVE ID : CVE-2023-28051**	https://www.dell.com/support/kbdoc/en-us/000211891/dsa-2023-221-dell-power-manager	A-DEL-POWE-200423/152
Product: streaming_data_platform					
Affected Version(s): * Up to (excluding) 1.4					
URL Redirection to Untrusted Site ('Open Redirect')	05-Apr-2023	5.4	Dell Streaming Data Platform prior to 1.4 contains Open Redirect vulnerability. An attacker with	https://www.dell.com/support/kbdoc/en-us/000204266/dsa-2022-258-dell-	A-DEL-STRE-200423/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges same as a legitimate user can phish the legitimate the user to redirect to malicious website leading to information disclosure and launch of phishing attacks. **CVE ID : CVE-2023-28069**	streaming-data-platform-security-update-for-multiple-third-party-component-vulnerabilities	
Product: trusted_device_agent					
Affected Version(s): * Up to (excluding) 5.3.0					
Incorrect Default Permissions	06-Apr-2023	7.8	Dell Trusted Device Agent, versions prior to 5.3.0, contain(s) an improper installation permissions vulnerability. An unauthenticated local attacker could potentially exploit this vulnerability, leading to escalated privileges. **CVE ID : CVE-2023-25542**	https://www.dell.com/support/kbdoc/en-us/000209461/dsa-2023-074	A-DEL-TRUS-200423/154
Vendor: devolutions					
Product: devolutions_gateway					
Affected Version(s): * Up to (excluding) 2023.1.2					
Uncontrolled Resource Consumption	02-Apr-2023	7.5	Uncontrolled resource consumption in the logging feature in Devolutions Gateway 2023.1.1 and earlier allows an attacker to cause a denial of service by filling up	https://devolutions.net/security/advisories/DEVO-2023-0007	A-DEV-DEVO-200423/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the disk and render the system unusable. **CVE ID : CVE-2023-1580**		
Product: devolutions_server					
Affected Version(s): * Up to (excluding) 2023.1.3.0					
Incorrect Authorization	02-Apr-2023	6.5	Permission bypass when importing or synchronizing entries in User vault in Devolutions Server 2022.3.13 and prior versions allows users with restricted rights to bypass entry permission via id collision. **CVE ID : CVE-2023-1603**	https://devolutions.net/security/advisories/DEVO-2023-0008	A-DEV-DEVO-200423/156
Product: remote_desktop_manager					
Affected Version(s): * Up to (excluding) 2023.1.10					
Incorrect Authorization	02-Apr-2023	6.5	Permission bypass when importing or synchronizing entries in User vault in Devolutions Remote Desktop Manager 2023.1.9 and prior versions allows users with restricted rights to bypass entry permission via id collision. **CVE ID : CVE-2023-1202**	https://devolutions.net/security/advisories/DEVO-2023-0008	A-DEV-REMO-200423/157
Insufficiently Protected Credentials	02-Apr-2023	6.5	Information disclosure in the user creation feature of a MSSQL data source in	https://devolutions.net/security/advisori	A-DEV-REMO-200423/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devolutions Remote Desktop Manager 2023.1.9 and below on Windows allows an attacker with access to the user interface to obtain sensitive information via the error message dialog that displays the password in clear text. **CVE ID : CVE-2023-1574**	es/DEVO-2023-0006	
Vendor: Docker					
Product: desktop					
Affected Version(s): 4.17.0					
Cleartext Transmission of Sensitive Information	06-Apr-2023	7.5	In Docker Desktop 4.17.x the Artifactory Integration falls back to sending registry credentials over plain HTTP if the HTTPS health check has failed. A targeted network sniffing attack can lead to a disclosure of sensitive information. Only users who have Access Experimental Features enabled and have logged in to a private registry are affected. **CVE ID : CVE-2023-1802**	N/A	A-DOC-DESK-200423/159
Affected Version(s): 4.17.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	06-Apr-2023	7.5	In Docker Desktop 4.17.x the Artifactory Integration falls back to sending registry credentials over plain HTTP if the HTTPS health check has failed. A targeted network sniffing attack can lead to a disclosure of sensitive information. Only users who have Access Experimental Features enabled and have logged in to a private registry are affected. **CVE ID : CVE-2023-1802**	N/A	A-DOC-DESK-200423/160
Vendor: dualspace					
Product: super_security					
Affected Version(s): 2.3.7					
Uncontrolled Resource Consumption	11-Apr-2023	7.5	An issue found in DUALSPACE Super Secuirty v.2.3.7 allows an attacker to cause a denial of service via the SharedPreference files. **CVE ID : CVE-2023-27191**	N/A	A-DUA-SUPE-200423/161
Vendor: dupeoff_project					
Product: dupeoff					
Affected Version(s): * Up to (including) 1.6					
Improper Neutralization of Input	03-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in	N/A	A-DUP-DUPE-200423/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			DupeOff.Com DupeOff plugin <= 1.6 versions. **CVE ID : CVE-2023-26529**		
Vendor: dynamic_transaction_queuing_system_project					
Product: dynamic_transaction_queuing_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	7.2	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter at /admin/ajax.php?action=login. **CVE ID : CVE-2023-26856**	N/A	A-DYN-DYNA-200423/163
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	7.2	An arbitrary file upload vulnerability in /admin/ajax.php?action=save_uploads of Dynamic Transaction Queuing System v1.0 allows attackers to execute arbitrary code via a crafted PHP file. **CVE ID : CVE-2023-26857**	N/A	A-DYN-DYNA-200423/164
Vendor: e4jconnect					
Product: vikrentcar					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Neutralization of Input During	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in E4J s.R.L. VikRentCar Car	N/A	A-E4J-VIKR-200423/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Rental Management System plugin <= 1.3.0 versions. **CVE ID : CVE-2023-23998**		
Vendor: earnings_and_expense_tracker_app_project					
Product: earnings_and_expense_tracker_app					
Affected Version(s): 1.0					
N/A	05-Apr-2023	7.5	A vulnerability was found in SourceCodester Earnings and Expense Tracker App 1.0. It has been classified as problematic. This affects an unknown part of the file index.php. The manipulation of the argument page leads to information disclosure. It is possible to initiate the attack remotely. The identifier VDB-224997 was assigned to this vulnerability. **CVE ID : CVE-2023-1858**	N/A	A-EAR-EARN-200423/166
Vendor: easy_panorama_project					
Product: easy_panorama					
Affected Version(s): * Up to (including) 1.1.4					
Improper Neutralization of Input During Web Page Generation	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in Leonardo Giacone Easy Panorama	N/A	A-EAS-EASY-200423/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			plugin <= 1.1.4 versions. **CVE ID : CVE-2023-23799**		
Vendor: edb-debugger_project					
Product: edb-debugger					
Affected Version(s): 1.3.0					
N/A	04-Apr-2023	5.5	An issue found in Eteran edb-debugger v.1.3.0 allows a local attacker to causea denial of service via the collect_symbols function in plugins/BinaryInfo/symbols.cpp. **CVE ID : CVE-2023-27734**	https://github.com/eteran/edb-debugger/pull/834/commits/32f325f4016e0090f76934320173581860f090be	A-EDB-EDB--200423/168
Vendor: ehuacui-bbs_project					
Product: ehuacui-bbs					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	8.2	Cross Site Scripting vulnerability found in Ehuacui BBS allows attackers to cause a denial of service via a crafted payload in the login parameter. **CVE ID : CVE-2023-27089**	N/A	A-EHU-EHUA-200423/169
Vendor: employee_payslip_generator_system_project					
Product: employee_payslip_generator_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During	02-Apr-2023	5.4	A vulnerability classified as problematic has been found in SourceCodester	N/A	A-EMP-EMPL-200423/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Employee Payslip Generator 1.0. Affected is an unknown function of the file /classes/Master.php ?f=save_position of the component Create News Handler. The manipulation of the argument name with the input <script>alert(document.cookie)</script> leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224748. **CVE ID : CVE-2023-1796**		
Vendor: envoyproxy					
Product: envoy					
Affected Version(s): * Up to (excluding) 1.22.9					
N/A	04-Apr-2023	9.8	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, escalation of privileges is possible when `failure_mode_allow:	https://github.com/envoyproxy/envoy/security/advisories/GHSA-9g5w-hqr3-w2ph	A-ENV-ENVO-200423/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			true` is configured for `ext_authz` filter. For affected components that are used for logging and/or visibility, requests may not be logged by the receiving service. When Envoy was configured to use ext_authz, ext_proc, tap, ratelimit filters, and grpc access log service and an http header with non-UTF-8 data was received, Envoy would generate an invalid protobuf message and send it to the configured service. The receiving service would typically generate an error when decoding the protobuf message. For ext_authz that was configured with ``failure_mode_allow: true``, the request would have been allowed in this case. For the other services, this could have resulted in other unforeseen errors such as a lack of visibility into requests. As of versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy by		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default sanitizes the values sent in gRPC service calls to be valid UTF-8, replacing data that is not valid UTF-8 with a `!` character. This behavioral change can be temporarily reverted by setting runtime guard `envoy.reloadable_features.service_sanitize_non_utf8_strings` to false. As a workaround, one may set `failure_mode_allow: false` for `ext_authz`. **CVE ID : CVE-2023-27488**		
N/A	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the client may bypass JSON Web Token (JWT) checks and forge fake original paths. The header `x-envoy-original-path` should be an internal header, but Envoy does not remove this header from the request at the beginning of request processing when it is	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5375-pq35-hf2g	A-ENV-ENVO-200423/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent from an untrusted client. The faked header would then be used for trace logs and grpc logs, as well as used in the URL used for `jwt_authn` checks if the `jwt_authn` filter is used, and any other upstream use of the x-envoy-original-path header. Attackers may forge a trusted `x-envoy-original-path` header. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 have patches for this issue. **CVE ID : CVE-2023-27487**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Compliant HTTP/1 service should reject malformed request lines. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, There is a possibility that non compliant HTTP/1 service may allow malformed requests, potentially leading to a bypass of security policies. This issue is fixed in versions	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5jmv-cw9p-f9rp	A-ENV-ENVO-200423/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9. **CVE ID : CVE-2023-27491**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy does not sanitize or escape request properties when generating request headers. This can lead to characters that are illegal in header values to be sent to the upstream service. In the worst case, it can cause upstream service to interpret the original request as two pipelined requests, possibly bypassing the intent of Envoy’s security policy. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. As a workaround, disable adding request headers based on the downstream request properties, such as downstream certificate properties.	https://github.com/envoyproxy/envoy/security/advisories/GHSA-w5w5-487h-qv8q	A-ENV-ENVO-200423/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27493		
N/A	04-Apr-2023	7.5	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the OAuth filter assumes that a \`state\` query param is present on any response that looks like an OAuth redirect response. Sending it a request with the URI path equivalent to the redirect path, without the \`state\` parameter, will lead to abnormal termination of Envoy process. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. The issue can also be mitigated by locking down OAuth traffic, disabling the filter, or by filtering traffic before it reaches the OAuth filter (e.g. via a lua script). **CVE ID : CVE-2023-27496**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-j79q-2g66-2xv5	A-ENV-ENVO-200423/175
Allocation of Resources Without	04-Apr-2023	6.5	Envoy is an open source edge and service proxy designed for cloud-	https://github.com/envoyproxy/envoy/security/advisor	A-ENV-ENVO-200423/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the Lua filter is vulnerable to denial of service. Attackers can send large request bodies for routes that have Lua filter enabled and trigger crashes. As of versions versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy no longer invokes the Lua coroutine if the filter has been reset. As a workaround for those whose Lua filter is buffering all requests/ responses, mitigate by using the buffer filter to avoid triggering the local reply in the Lua filter. **CVE ID : CVE-2023-27492**	ies/GHSA-wpc2-2jp6-ppg2	
Affected Version(s): From (including) 1.23.0 Up to (excluding) 1.23.6					
N/A	04-Apr-2023	9.8	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, escalation of privileges is possible when `failure_mode_allow:	https://github.com/envoyproxy/envoy/security/advisories/GHSA-9g5w-hqr3-w2ph	A-ENV-ENVO-200423/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			true` is configured for `ext_authz` filter. For affected components that are used for logging and/or visibility, requests may not be logged by the receiving service. When Envoy was configured to use ext_authz, ext_proc, tap, ratelimit filters, and grpc access log service and an http header with non-UTF-8 data was received, Envoy would generate an invalid protobuf message and send it to the configured service. The receiving service would typically generate an error when decoding the protobuf message. For ext_authz that was configured with ``failure_mode_allow: true``, the request would have been allowed in this case. For the other services, this could have resulted in other unforeseen errors such as a lack of visibility into requests. As of versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy by		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default sanitizes the values sent in gRPC service calls to be valid UTF-8, replacing data that is not valid UTF-8 with a `!` character. This behavioral change can be temporarily reverted by setting runtime guard `envoy.reloadable_features.service_sanitize_non_utf8_strings` to false. As a workaround, one may set `failure_mode_allow: false` for `ext_authz`. **CVE ID : CVE-2023-27488**		
N/A	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the client may bypass JSON Web Token (JWT) checks and forge fake original paths. The header `x-envoy-original-path` should be an internal header, but Envoy does not remove this header from the request at the beginning of request processing when it is	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5375-pq35-hf2g	A-ENV-ENVO-200423/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent from an untrusted client. The faked header would then be used for trace logs and grpc logs, as well as used in the URL used for `jwt_authn` checks if the `jwt_authn` filter is used, and any other upstream use of the x-envoy-original-path header. Attackers may forge a trusted `x-envoy-original-path` header. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 have patches for this issue. **CVE ID : CVE-2023-27487**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Compliant HTTP/1 service should reject malformed request lines. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, There is a possibility that non compliant HTTP/1 service may allow malformed requests, potentially leading to a bypass of security policies. This issue is fixed in versions	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5jmv-cw9p-f9rp	A-ENV-ENVO-200423/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9. **CVE ID : CVE-2023-27491**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy does not sanitize or escape request properties when generating request headers. This can lead to characters that are illegal in header values to be sent to the upstream service. In the worst case, it can cause upstream service to interpret the original request as two pipelined requests, possibly bypassing the intent of Envoy's security policy. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. As a workaround, disable adding request headers based on the downstream request properties, such as downstream certificate properties.	https://github.com/envoyproxy/envoy/security/advisories/GHSA-w5w5-487h-qv8q	A-ENV-ENVO-200423/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27493		
N/A	04-Apr-2023	7.5	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the OAuth filter assumes that a `state` query param is present on any response that looks like an OAuth redirect response. Sending it a request with the URI path equivalent to the redirect path, without the `state` parameter, will lead to abnormal termination of Envoy process. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. The issue can also be mitigated by locking down OAuth traffic, disabling the filter, or by filtering traffic before it reaches the OAuth filter (e.g. via a lua script). **CVE ID : CVE-2023-27496**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-j79q-2g66-2xv5	A-ENV-ENVO-200423/181
Allocation of Resources Without	04-Apr-2023	6.5	Envoy is an open source edge and service proxy designed for cloud-	https://github.com/envoyproxy/envoy/security/advisor	A-ENV-ENVO-200423/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the Lua filter is vulnerable to denial of service. Attackers can send large request bodies for routes that have Lua filter enabled and trigger crashes. As of versions versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy no longer invokes the Lua coroutine if the filter has been reset. As a workaround for those whose Lua filter is buffering all requests/ responses, mitigate by using the buffer filter to avoid triggering the local reply in the Lua filter. **CVE ID : CVE-2023-27492**	ies/GHSA-wpc2-2jp6-ppg2	
Affected Version(s): From (including) 1.24.0 Up to (excluding) 1.24.4					
N/A	04-Apr-2023	9.8	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, escalation of privileges is possible when `failure_mode_allow:	https://github.com/envoyproxy/envoy/security/advisories/GHSA-9g5w-hqr3-w2ph	A-ENV-ENVO-200423/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	true` is configured for `ext_authz` filter. For affected components that are used for logging and/or visibility, requests may not be logged by the receiving service. When Envoy was configured to use ext_authz, ext_proc, tap, ratelimit filters, and grpc access log service and an http header with non-UTF-8 data was received, Envoy would generate an invalid protobuf message and send it to the configured service. The receiving service would typically generate an error when decoding the protobuf message. For ext_authz that was configured with ``failure_mode_allow: true``, the request would have been allowed in this case. For the other services, this could have resulted in other unforeseen errors such as a lack of visibility into requests. As of versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy by		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default sanitizes the values sent in gRPC service calls to be valid UTF-8, replacing data that is not valid UTF-8 with a `!` character. This behavioral change can be temporarily reverted by setting runtime guard `envoy.reloadable_features.service_sanitize_non_utf8_strings` to false. As a workaround, one may set `failure_mode_allow: false` for `ext_authz`. **CVE ID : CVE-2023-27488**		
N/A	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the client may bypass JSON Web Token (JWT) checks and forge fake original paths. The header `x-envoy-original-path` should be an internal header, but Envoy does not remove this header from the request at the beginning of request processing when it is	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5375-pq35-hf2g	A-ENV-ENVO-200423/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent from an untrusted client. The faked header would then be used for trace logs and grpc logs, as well as used in the URL used for `jwt_authn` checks if the `jwt_authn` filter is used, and any other upstream use of the x-envoy-original-path header. Attackers may forge a trusted `x-envoy-original-path` header. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 have patches for this issue. **CVE ID : CVE-2023-27487**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Compliant HTTP/1 service should reject malformed request lines. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, There is a possibility that non compliant HTTP/1 service may allow malformed requests, potentially leading to a bypass of security policies. This issue is fixed in versions	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5jmv-cw9p-f9rp	A-ENV-ENVO-200423/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9. **CVE ID : CVE-2023-27491**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy does not sanitize or escape request properties when generating request headers. This can lead to characters that are illegal in header values to be sent to the upstream service. In the worst case, it can cause upstream service to interpret the original request as two pipelined requests, possibly bypassing the intent of Envoy's security policy. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. As a workaround, disable adding request headers based on the downstream request properties, such as downstream certificate properties.	https://github.com/envoyproxy/envoy/security/advisories/GHSA-w5w5-487h-qv8q	A-ENV-ENVO-200423/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27493		
N/A	04-Apr-2023	7.5	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the OAuth filter assumes that a \`state\` query param is present on any response that looks like an OAuth redirect response. Sending it a request with the URI path equivalent to the redirect path, without the \`state\` parameter, will lead to abnormal termination of Envoy process. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. The issue can also be mitigated by locking down OAuth traffic, disabling the filter, or by filtering traffic before it reaches the OAuth filter (e.g. via a lua script). **CVE ID : CVE-2023-27496**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-j79q-2g66-2xv5	A-ENV-ENVO-200423/187
Allocation of Resources Without	04-Apr-2023	6.5	Envoy is an open source edge and service proxy designed for cloud-	https://github.com/envoyproxy/envoy/security/advisor	A-ENV-ENVO-200423/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the Lua filter is vulnerable to denial of service. Attackers can send large request bodies for routes that have Lua filter enabled and trigger crashes. As of versions versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy no longer invokes the Lua coroutine if the filter has been reset. As a workaround for those whose Lua filter is buffering all requests/ responses, mitigate by using the buffer filter to avoid triggering the local reply in the Lua filter. **CVE ID : CVE-2023-27492**	ies/GHSA-wpc2-2jp6-ppg2	
Affected Version(s): From (including) 1.25.0 Up to (excluding) 1.25.3					
N/A	04-Apr-2023	9.8	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, escalation of privileges is possible when `failure_mode_allow:	https://github.com/envoyproxy/envoy/security/advisories/GHSA-9g5w-hqr3-w2ph	A-ENV-ENVO-200423/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟥	true` is configured for `ext_authz` filter. For affected components that are used for logging and/or visibility, requests may not be logged by the receiving service. When Envoy was configured to use ext_authz, ext_proc, tap, ratelimit filters, and grpc access log service and an http header with non-UTF-8 data was received, Envoy would generate an invalid protobuf message and send it to the configured service. The receiving service would typically generate an error when decoding the protobuf message. For ext_authz that was configured with ``failure_mode_allow: true``, the request would have been allowed in this case. For the other services, this could have resulted in other unforeseen errors such as a lack of visibility into requests. As of versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy by		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			default sanitizes the values sent in gRPC service calls to be valid UTF-8, replacing data that is not valid UTF-8 with a `!` character. This behavioral change can be temporarily reverted by setting runtime guard `envoy.reloadable_features.service_sanitize_non_utf8_strings` to false. As a workaround, one may set `failure_mode_allow: false` for `ext_authz`. **CVE ID : CVE-2023-27488**		
N/A	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the client may bypass JSON Web Token (JWT) checks and forge fake original paths. The header `x-envoy-original-path` should be an internal header, but Envoy does not remove this header from the request at the beginning of request processing when it is	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5375-pq35-hf2g	A-ENV-ENVO-200423/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent from an untrusted client. The faked header would then be used for trace logs and grpc logs, as well as used in the URL used for `jwt_authn` checks if the `jwt_authn` filter is used, and any other upstream use of the x-envoy-original-path header. Attackers may forge a trusted `x-envoy-original-path` header. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 have patches for this issue. **CVE ID : CVE-2023-27487**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Compliant HTTP/1 service should reject malformed request lines. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, There is a possibility that non compliant HTTP/1 service may allow malformed requests, potentially leading to a bypass of security policies. This issue is fixed in versions	https://github.com/envoyproxy/envoy/security/advisories/GHSA-5jmv-cw9p-f9rp	A-ENV-ENVO-200423/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9. **CVE ID : CVE-2023-27491**		
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	04-Apr-2023	9.1	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy does not sanitize or escape request properties when generating request headers. This can lead to characters that are illegal in header values to be sent to the upstream service. In the worst case, it can cause upstream service to interpret the original request as two pipelined requests, possibly bypassing the intent of Envoy's security policy. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. As a workaround, disable adding request headers based on the downstream request properties, such as downstream certificate properties.	https://github.com/envoyproxy/envoy/security/advisories/GHSA-w5w5-487h-qv8q	A-ENV-ENVO-200423/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27493		
N/A	04-Apr-2023	7.5	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the OAuth filter assumes that a `state` query param is present on any response that looks like an OAuth redirect response. Sending it a request with the URI path equivalent to the redirect path, without the `state` parameter, will lead to abnormal termination of Envoy process. Versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9 contain a patch. The issue can also be mitigated by locking down OAuth traffic, disabling the filter, or by filtering traffic before it reaches the OAuth filter (e.g. via a lua script). **CVE ID : CVE-2023-27496**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-j79q-2g66-2xv5	A-ENV-ENVO-200423/193
Allocation of Resources Without	04-Apr-2023	6.5	Envoy is an open source edge and service proxy designed for cloud-	https://github.com/envoyproxy/envoy/security/advisor	A-ENV-ENVO-200423/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			native applications. Prior to versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, the Lua filter is vulnerable to denial of service. Attackers can send large request bodies for routes that have Lua filter enabled and trigger crashes. As of versions versions 1.26.0, 1.25.3, 1.24.4, 1.23.6, and 1.22.9, Envoy no longer invokes the Lua coroutine if the filter has been reset. As a workaround for those whose Lua filter is buffering all requests/ responses, mitigate by using the buffer filter to avoid triggering the local reply in the Lua filter. **CVE ID : CVE-2023-27492**	ies/GHSA-wpc2-2jp6-ppg2	
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): * Up to (including) 1.5.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	A vulnerability, which was classified as problematic, has been found in EyouCMS up to 1.5.4. Affected by this issue is some unknown functionality of the file login.php. The	N/A	A-EYO-EYOU-200423/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument typename leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-224750 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1798**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	A vulnerability, which was classified as problematic, was found in EyouCMS up to 1.5.4. This affects an unknown part of the file login.php. The manipulation of the argument tag_tag leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224751. **CVE ID : CVE-2023-1799**	N/A	A-EYO-EYOU-200423/196
Vendor: fernus					
Product: learning_management_systems					
Affected Version(s): * Up to (excluding) 23.04.03					
Unrestricted Upload of File with	04-Apr-2023	9.8	Unrestricted Upload of File with Dangerous Type	N/A	A-FER-LEAR-200423/197

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			vulnerability in Fernus Informatics LMS allows OS Command Injection, Server Side Include (SSI) Injection.This issue affects LMS: before 23.04.03. **CVE ID : CVE-2023-1728**		
Vendor: firefly-iii					
Product: firefly_iii					
Affected Version(s): * Up to (excluding) 6.0.0					
Insufficient Session Expiration	05-Apr-2023	9.8	Insufficient Session Expiration in GitHub repository firefly-iii/firefly-iii prior to 6. **CVE ID : CVE-2023-1788**	https://huntr.dev/bounties/79323c9e-e0e5-48ef-bd19-d0b09587ccb2, https://github.com/firefly-iii/firefly-iii/commit/68f398f97cbe1870fc098d8460bf903b9c3fab30	A-FIR-FIRE-200423/198
Affected Version(s): * Up to (excluding) 5.7.18					
Improper Input Validation	01-Apr-2023	9.8	Improper Input Validation in GitHub repository firefly-iii/firefly-iii prior to 6.0.0. **CVE ID : CVE-2023-1789**	https://github.com/firefly-iii/firefly-iii/commit/6b05c0fbd3e8c40ae9b24dc2698821786fccf0c5, https://huntr.dev/bounties/	A-FIR-FIRE-200423/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2c3489f7-6b84-48f8-9368-9cea67cf373d	
Affected Version(s): 5.8.0					
Improper Input Validation	01-Apr-2023	9.8	Improper Input Validation in GitHub repository firefly-iii/firefly-iii prior to 6.0.0. **CVE ID : CVE-2023-1789**	https://github.com/firefly-iii/firefly-iii/commit/6b05c0fbd3e8c40ae9b24dc2698821786fccf0c5, https://huntr.dev/bounties/2c3489f7-6b84-48f8-9368-9cea67cf373d	A-FIR-FIRE-200423/200
Affected Version(s): 6.0.0					
Insufficient Session Expiration	05-Apr-2023	9.8	Insufficient Session Expiration in GitHub repository firefly-iii/firefly-iii prior to 6. **CVE ID : CVE-2023-1788**	https://huntr.dev/bounties/79323c9e-e0e5-48ef-bd19-d0b09587ccb2, https://github.com/firefly-iii/firefly-iii/commit/68f398f97cbe1870fc098d8460bf903b9c3fab30	A-FIR-FIRE-200423/201
Improper Input Validation	01-Apr-2023	9.8	Improper Input Validation in GitHub repository firefly-iii/firefly-iii prior to 6.0.0. **CVE ID : CVE-2023-1789**	https://github.com/firefly-iii/firefly-iii/commit/6b05c0fbd3e8c40ae9b24dc2698821786fccf	A-FIR-FIRE-200423/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0c5, https://huntr.dev/bounties/2c3489f7-6b84-48f8-9368-9cea67cf373d	
Vendor: flippercode					
Product: google_map					
Affected Version(s): * Up to (excluding) 4.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	5.4	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in flippercode WordPress Plugin for Google Maps – WP MAPS plugin <= 4.3.9 versions. **CVE ID : CVE-2023-23878**	N/A	A-FLI-GOOG-200423/203
Vendor: fluentforms					
Product: contact_form					
Affected Version(s): * Up to (excluding) 4.3.25					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	The Contact Form Plugin WordPress plugin before 4.3.25 does not properly sanitize and escape the srcdoc attribute in iframes in it's custom HTML field type, allowing a logged in user with roles as low as contributor to inject arbitrary javascript into a form which will trigger for any visitor to the form or	N/A	A-FLU-CONT-200423/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			admins previewing or editing the form. **CVE ID : CVE-2023-0546**		
Vendor: followmedarling					
Product: spotify-play-button-for-wordpress					
Affected Version(s): * Up to (excluding) 2.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Jonk @ Follow me Darling Sp*tify Play Button for WordPress plugin <= 2.05 versions. **CVE ID : CVE-2023-26536**	N/A	A-FOL-SPOT-200423/205
Affected Version(s): * Up to (including) 2.07					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	4.8	The Sp*tify Play Button for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 2.07 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This	N/A	A-FOL-SPOT-200423/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-1840**		
Vendor: fullworksplugins					
Product: quick_contact_form					
Affected Version(s): * Up to (including) 8.0.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Contact Form plugin <= 8.0.3.1 versions. **CVE ID : CVE-2023-23885**	N/A	A-FUL-QUIC-200423/207
Product: quick_event_manager					
Affected Version(s): * Up to (excluding) 9.7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Event Manager plugin <= 9.7.4 versions. **CVE ID : CVE-2023-23979**	N/A	A-FUL-QUIC-200423/208
Product: quick_paypal_payments					
Affected Version(s): * Up to (excluding) 5.7.26					
Improper Neutralization of Input During Web Page Generation	07-Apr-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Fullworks Quick Paypal Payments plugin <= 5.7.25 versions.	N/A	A-FUL-QUIC-200423/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-25713**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in Fullworks Quick Paypal Payments plugin <= 5.7.25 versions. **CVE ID : CVE-2023-25702**	N/A	A-FUL-QUIC-200423/210
Vendor: gadget_works_online_ordering_system_project					
Product: gadget_works_online_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	6.1	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/products/index.php of the component GET Parameter Handler. The manipulation of the argument view with the input <script>alert(666)</script> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-GAD-GADG-200423/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-224747. **CVE ID : CVE-2023-1795**		
Vendor: gdidees					
Product: gdidees_cms					
Affected Version(s): 3.9.1					
Unrestricted Upload of File with Dangerous Type	10-Apr-2023	9.8	An arbitrary file upload vulnerability in the upload function of GDidees CMS 3.9.1 allows attackers to execute arbitrary code via a crafted file. **CVE ID : CVE-2023-27178**	N/A	A-GDI-GDID-200423/212
Affected Version(s): * Up to (including) 3.9.1					
Unrestricted Upload of File with Dangerous Type	11-Apr-2023	7.5	GDidees CMS v3.9.1 and lower was discovered to contain an arbitrary file download vulenrability via the filename parameter at /_admin/imgdownload.php. **CVE ID : CVE-2023-27179**	N/A	A-GDI-GDID-200423/213
N/A	07-Apr-2023	7.5	GDidees CMS v3.9.1 was discovered to contain a source code disclosure vulnerability by the backup feature which is accessible via /_admin/backup.php.	N/A	A-GDI-GDID-200423/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27180		
Vendor: genetech					
Product: security_center					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	8.8	SQL Injection in the Hardware Inventory report of Security Center 5.11.2. **CVE ID : CVE-2023-1522**	https://www.genetec.com/blog/data-protection/high-severity-vulnerability-affecting-the-hardware-inventory-report-task-of-security-center	A-GEN-SECU-200423/215
Affected Version(s): 5.11.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	8.8	SQL Injection in the Hardware Inventory report of Security Center 5.11.2. **CVE ID : CVE-2023-1522**	https://www.genetec.com/blog/data-protection/high-severity-vulnerability-affecting-the-hardware-inventory-report-task-of-security-center	A-GEN-SECU-200423/216
Vendor: Github					
Product: enterprise_server					
Affected Version(s): * Up to (excluding) 3.4.18					
Improper Authentication	07-Apr-2023	5.3	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor	N/A	A-GIT-ENTE-200423/217

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to modify other users' secret gists by authenticating through an SSH certificate authority. To do so, a user had to know the secret gist’s URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23761**		
Incorrect Comparison	07-Apr-2023	5.3	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff. To do so, an attacker would need write access to the repository and be able to correctly guess the target branch before it’s created by the code maintainer. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9	N/A	A-GIT-ENTE-200423/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23762**		
Affected Version(s): 3.8.0					
Improper Authentication	07-Apr-2023	5.3	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to modify other users' secret gists by authenticating through an SSH certificate authority. To do so, a user had to know the secret gist's URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23761**	N/A	A-GIT-ENTE-200423/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Comparison	07-Apr-2023	5.3	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff. To do so, an attacker would need write access to the repository and be able to correctly guess the target branch before it's created by the code maintainer. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23762**	N/A	A-GIT-ENTE-200423/220
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.15					
Improper Authentication	07-Apr-2023	5.3	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to modify other users' secret gists by authenticating through an SSH	N/A	A-GIT-ENTE-200423/221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certificate authority. To do so, a user had to know the secret gist's URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23761**		
Incorrect Comparison	07-Apr-2023	5.3	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff. To do so, an attacker would need write access to the repository and be able to correctly guess the target branch before it's created by the code maintainer. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This	N/A	A-GIT-ENTE-200423/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23762**		
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.11					
Improper Authentication	07-Apr-2023	5.3	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to modify other users' secret gists by authenticating through an SSH certificate authority. To do so, a user had to know the secret gist's URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23761**	N/A	A-GIT-ENTE-200423/223
Incorrect Comparison	07-Apr-2023	5.3	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit	N/A	A-GIT-ENTE-200423/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			smuggling by displaying an incorrect diff. To do so, an attacker would need write access to the repository and be able to correctly guess the target branch before it's created by the code maintainer. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23762**		
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.8					
Improper Authentication	07-Apr-2023	5.3	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed an unauthorized actor to modify other users' secret gists by authenticating through an SSH certificate authority. To do so, a user had to know the secret gist's URL. This vulnerability affected all versions of	N/A	A-GIT-ENTE-200423/225

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23761**		
Incorrect Comparison	07-Apr-2023	5.3	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff. To do so, an attacker would need write access to the repository and be able to correctly guess the target branch before it's created by the code maintainer. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.9 and was fixed in versions 3.4.18, 3.5.15, 3.6.11, 3.7.8, and 3.8.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-23762**	N/A	A-GIT-ENTE-200423/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): 15.10.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	9.8	An issue was identified in GitLab CE/EE affecting all versions from 1.0 prior to 15.8.5, 15.9 prior to 15.9.4, and 15.10 prior to 15.10.1 where non-printable characters gets copied from clipboard, allowing unexpected commands to be executed on victim machine. **CVE ID : CVE-2023-1708**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1708.json	A-GIT-GITL-200423/227
N/A	05-Apr-2023	7.5	A denial of service condition exists in the Prometheus server bundled with GitLab affecting all versions from 11.10 to 15.8.5, 15.9 to 15.9.4 and 15.10 to 15.10.1. **CVE ID : CVE-2023-1733**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1733.json	A-GIT-GITL-200423/228
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	An issue has been discovered in GitLab affecting all versions starting from 15.6 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. An XSS was possible via a malicious email	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0523.json	A-GIT-GITL-200423/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address for certain instances. **CVE ID : CVE-2023-0523**		
Incorrect Authorization	05-Apr-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 13.6 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1, allowing to read environment names supposed to be restricted to project memebers only. **CVE ID : CVE-2023-0319**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0319.json	A-GIT-GITL-200423/230
Missing Authorization	05-Apr-2023	5.3	Improper authorization in Gitlab EE affecting all versions from 12.3.0 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 allows an unauthorized access to security reports in MR. **CVE ID : CVE-2023-1167**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1167.json	A-GIT-GITL-200423/231
N/A	05-Apr-2023	5.3	A sensitive information disclosure vulnerability in GitLab affecting all	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-	A-GIT-GITL-200423/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions from 15.0 prior to 15.8.5, 15.9 prior to 15.9.4 and 15.10 prior to 15.10.1 allows an attacker to view the count of internal notes for a given issue. **CVE ID : CVE-2023-1710**	2023-1710.json	
N/A	05-Apr-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. A search timeout could be triggered if a specific HTML payload was used in the issue description. **CVE ID : CVE-2023-1787**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1787.json	A-GIT-GITL-200423/233
N/A	05-Apr-2023	4.9	An information disclosure vulnerability has been discovered in GitLab EE/CE affecting all versions starting from 11.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 will allow an admin to leak password from	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1098.json	A-GIT-GITL-200423/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repository mirror configuration. **CVE ID : CVE-2023-1098**		
N/A	05-Apr-2023	4.6	An issue has been discovered in GitLab affecting all versions starting from 8.1 to 15.8.5, and from 15.9 to 15.9.4, and from 15.10 to 15.10.1. It was possible to add a branch with an ambiguous name that could be used to social engineer users. **CVE ID : CVE-2023-0450**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0450.json	A-GIT-GITL-200423/235
Incorrect Authorization	05-Apr-2023	4.3	An issue has been discovered in GitLab affecting all versions from 15.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. Due to improper permissions checks it was possible for an unauthorised user to remove an issue from an epic. **CVE ID : CVE-2023-1071**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1071.json	A-GIT-GITL-200423/236
Incorrect Authorization	05-Apr-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 15.9 before 15.9.4, all	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-	A-GIT-GITL-200423/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 15.10 before 15.10.1. It was possible for an unauthorised user to add child epics linked to victim's epic in an unrelated group. **CVE ID : CVE-2023-1417**	2023-1417.json	
N/A	05-Apr-2023	3.8	An issue has been discovered in GitLab affecting versions starting from 15.1 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. A maintainer could modify a webhook URL to leak masked webhook secrets by adding a new parameter to the url. This addresses an incomplete fix for CVE-2022-4342. **CVE ID : CVE-2023-0838**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0838.json	A-GIT-GITL-200423/238
Affected Version(s): From (including) 1.0.0 Up to (excluding) 15.8.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	9.8	An issue was identified in GitLab CE/EE affecting all versions from 1.0 prior to 15.8.5, 15.9 prior to 15.9.4, and 15.10 prior to 15.10.1 where non-printable characters gets copied from clipboard, allowing unexpected	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1708.json	A-GIT-GITL-200423/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands to be executed on victim machine. **CVE ID : CVE-2023-1708**		
Affected Version(s): From (including) 11.10.0 Up to (excluding) 15.8.5					
N/A	05-Apr-2023	7.5	A denial of service condition exists in the Prometheus server bundled with GitLab affecting all versions from 11.10 to 15.8.5, 15.9 to 15.9.4 and 15.10 to 15.10.1. **CVE ID : CVE-2023-1733**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1733.json	A-GIT-GITL-200423/240
Affected Version(s): From (including) 11.5.0 Up to (excluding) 15.8.5					
N/A	05-Apr-2023	4.9	An information disclosure vulnerability has been discovered in GitLab EE/CE affecting all versions starting from 11.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 will allow an admin to leak password from repository mirror configuration. **CVE ID : CVE-2023-1098**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1098.json	A-GIT-GITL-200423/241
Affected Version(s): From (including) 12.3.0 Up to (excluding) 15.8.5					
Missing Authorization	05-Apr-2023	5.3	Improper authorization in Gitlab EE affecting all	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-200423/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions from 12.3.0 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 allows an unauthorized access to security reports in MR. **CVE ID : CVE-2023-1167**	/blob/master/2023/CVE-2023-1167.json	
Affected Version(s): From (including) 13.6.0 Up to (excluding) 15.8.5					
Incorrect Authorization	05-Apr-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 13.6 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1, allowing to read environment names supposed to be restricted to project memebers only. **CVE ID : CVE-2023-0319**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0319.json	A-GIT-GITL-200423/243
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.8.5					
N/A	05-Apr-2023	5.3	A sensitive information disclosure vulnerability in GitLab affecting all versions from 15.0 prior to 15.8.5, 15.9 prior to 15.9.4 and 15.10 prior to 15.10.1 allows an	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1710.json	A-GIT-GITL-200423/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to view the count of internal notes for a given issue. **CVE ID : CVE-2023-1710**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.8.5					
N/A	05-Apr-2023	3.8	An issue has been discovered in GitLab affecting versions starting from 15.1 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. A maintainer could modify a webhook URL to leak masked webhook secrets by adding a new parameter to the url. This addresses an incomplete fix for CVE-2022-4342. **CVE ID : CVE-2023-0838**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0838.json	A-GIT-GITL-200423/245
Affected Version(s): From (including) 15.5.0 Up to (excluding) 15.8.5					
Incorrect Authorization	05-Apr-2023	4.3	An issue has been discovered in GitLab affecting all versions from 15.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. Due to improper permissions checks it was possible for an unauthorised user to remove an issue from an epic.	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1071.json	A-GIT-GITL-200423/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1071		
Affected Version(s): From (including) 15.6.0 Up to (excluding) 15.8.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	An issue has been discovered in GitLab affecting all versions starting from 15.6 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. An XSS was possible via a malicious email address for certain instances. **CVE ID : CVE-2023-0523**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0523.json	A-GIT-GITL-200423/247
Affected Version(s): From (including) 15.6.0 Up to (including) 15.8.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	An issue has been discovered in GitLab affecting all versions starting from 15.6 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. An XSS was possible via a malicious email address for certain instances. **CVE ID : CVE-2023-0523**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0523.json	A-GIT-GITL-200423/248
Affected Version(s): From (including) 15.9.0 Up to (excluding) 15.9.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	9.8	An issue was identified in GitLab CE/EE affecting all versions from 1.0 prior to 15.8.5, 15.9 prior to 15.9.4, and 15.10 prior to 15.10.1 where non-printable characters gets copied from	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1708.json	A-GIT-GITL-200423/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			clipboard, allowing unexpected commands to be executed on victim machine. **CVE ID : CVE-2023-1708**		
N/A	05-Apr-2023	7.5	A denial of service condition exists in the Prometheus server bundled with GitLab affecting all versions from 11.10 to 15.8.5, 15.9 to 15.9.4 and 15.10 to 15.10.1. **CVE ID : CVE-2023-1733**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1733.json	A-GIT-GITL-200423/250
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	An issue has been discovered in GitLab affecting all versions starting from 15.6 before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. An XSS was possible via a malicious email address for certain instances. **CVE ID : CVE-2023-0523**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0523.json	A-GIT-GITL-200423/251
Incorrect Authorization	05-Apr-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 13.6 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1, allowing to read	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0319.json	A-GIT-GITL-200423/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			environment names supposed to be restricted to project memebers only. **CVE ID : CVE-2023-0319**		
Missing Authorization	05-Apr-2023	5.3	Improper authorization in Gitlab EE affecting all versions from 12.3.0 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 allows an unauthorized access to security reports in MR. **CVE ID : CVE-2023-1167**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1167.json	A-GIT-GITL-200423/253
N/A	05-Apr-2023	5.3	A sensitive information disclosure vulnerability in GitLab affecting all versions from 15.0 prior to 15.8.5, 15.9 prior to 15.9.4 and 15.10 prior to 15.10.1 allows an attacker to view the count of internal notes for a given issue. **CVE ID : CVE-2023-1710**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1710.json	A-GIT-GITL-200423/254
N/A	05-Apr-2023	5.3	An issue has been discovered in GitLab affecting all versions starting from 15.9	https://gitlab.com/gitlab-org/cves/-/blob/master	A-GIT-GITL-200423/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 15.9.4, all versions starting from 15.10 before 15.10.1. A search timeout could be triggered if a specific HTML payload was used in the issue description. **CVE ID : CVE-2023-1787**	/2023/CVE-2023-1787.json	
N/A	05-Apr-2023	4.9	An information disclosure vulnerability has been discovered in GitLab EE/CE affecting all versions starting from 11.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1 will allow an admin to leak password from repository mirror configuration. **CVE ID : CVE-2023-1098**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1098.json	A-GIT-GITL-200423/256
N/A	05-Apr-2023	4.6	An issue has been discovered in GitLab affecting all versions starting from 8.1 to 15.8.5, and from 15.9 to 15.9.4, and from 15.10 to 15.10.1. It was possible to add a branch with an ambiguous name that could be used to	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0450.json	A-GIT-GITL-200423/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			social engineer users. **CVE ID : CVE-2023-0450**		
Incorrect Authorization	05-Apr-2023	4.3	An issue has been discovered in GitLab affecting all versions from 15.5 before 15.8.5, all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. Due to improper permissions checks it was possible for an unauthorised user to remove an issue from an epic. **CVE ID : CVE-2023-1071**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1071.json	A-GIT-GITL-200423/258
Incorrect Authorization	05-Apr-2023	4.3	An issue has been discovered in GitLab affecting all versions starting from 15.9 before 15.9.4, all versions starting from 15.10 before 15.10.1. It was possible for an unauthorised user to add child epics linked to victim's epic in an unrelated group. **CVE ID : CVE-2023-1417**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-1417.json	A-GIT-GITL-200423/259
N/A	05-Apr-2023	3.8	An issue has been discovered in GitLab affecting versions starting from 15.1	https://gitlab.com/gitlab-org/cves/-/blob/master	A-GIT-GITL-200423/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 15.8.5, 15.9 before 15.9.4, and 15.10 before 15.10.1. A maintainer could modify a webhook URL to leak masked webhook secrets by adding a new parameter to the url. This addresses an incomplete fix for CVE-2022-4342. **CVE ID : CVE-2023-0838**	/2023/CVE-2023-0838.json	
Affected Version(s): From (including) 8.1.0 Up to (excluding) 15.8.5					
N/A	05-Apr-2023	4.6	An issue has been discovered in GitLab affecting all versions starting from 8.1 to 15.8.5, and from 15.9 to 15.9.4, and from 15.10 to 15.10.1. It was possible to add a branch with an ambiguous name that could be used to social engineer users. **CVE ID : CVE-2023-0450**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-0450.json	A-GIT-GITL-200423/261
Vendor: Glpi-project					
Product: glpi					
Affected Version(s): From (including) 0.50 Up to (excluding) 9.5.13					
Improper Neutralization of Special Elements used in an SQL Command	05-Apr-2023	8.1	GLPI is a free asset and IT management software package. Starting in version 0.50 and prior to versions 9.5.13 and 10.0.7, a SQL Injection	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/s	A-GLP-GLPI-200423/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			vulnerability allow users with access rights to statistics or reports to extract all data from database and, in some cases, write a webshell on the server. Versions 9.5.13 and 10.0.7 contain a patch for this issue. As a workaround, remove `Assistance > Statistics` and `Tools > Reports` read rights from every user. **CVE ID : CVE-2023-28838**	ecurity/advisories/GHSA-2c7r-gf38-358f, https://github.com/glpi-project/glpi/releases/tag/10.0.7	
Affected Version(s): From (including) 0.60 Up to (excluding) 9.5.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	4.8	GLPI is a free asset and IT management software package. Starting in version 0.60 and prior to versions 9.5.13 and 10.0.7, a vulnerability allows an administrator to create a malicious external link. This issue is fixed in versions 9.5.13 and 10.0.7. **CVE ID : CVE-2023-28636**	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/releases/tag/10.0.7, https://github.com/glpi-project/glpi/security/advisories/GHSA-55pm-mc2m-pq46	A-GLP-GLPI-200423/263
Affected Version(s): From (including) 0.83 Up to (excluding) 9.5.13					
Improper Authorization	05-Apr-2023	8.8	GLPI is a free asset and IT management software package. Starting in version	https://github.com/glpi-project/glpi/releases/tag/9.	A-GLP-GLPI-200423/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.83 and prior to versions 9.5.13 and 10.0.7, a user who has the Technician profile could see and generate a Personal token for a Super-Admin. Using such token it is possible to negotiate a GLPI session and hijack the Super-Admin account, resulting in a Privilege Escalation. Versions 9.5.13 and 10.0.7 contain a patch for this issue. **CVE ID : CVE-2023-28634**	5.13, https://github.com/glpi-project/glpi/releases/tag/10.0.7, https://github.com/glpi-project/glpi/security/advisories/GHSA-4279-rxmh-gf39	
Improper Privilege Management	05-Apr-2023	8.1	GLPI is a free asset and IT management software package. Starting in version 0.83 and prior to versions 9.5.13 and 10.0.7, an authenticated user can modify emails of any user, and can therefore takeover another user account through the "forgotten password" feature. By modifying emails, the user can also receive sensitive data through GLPI notifications. Versions 9.5.13 and 10.0.7 contain a patch for this issue.	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/releases/tag/10.0.7, https://github.com/glpi-project/glpi/security/advisories/GHSA-7pwm-pg76-3q9x	A-GLP-GLPI-200423/265

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			As a workaround, account takeover can be prevented by deactivating all notifications related to `Forgotten password?` event. However, it will not prevent unauthorized modification of any user emails. **CVE ID : CVE-2023-28632**		
Affected Version(s): From (including) 0.84 Up to (excluding) 9.5.13					
Server-Side Request Forgery (SSRF)	05-Apr-2023	5.4	GLPI is a free asset and IT management software package. Starting in version 0.84 and prior to versions 9.5.13 and 10.0.7, usage of RSS feeds is subject to server-side request forgery (SSRF). In case the remote address is not a valid RSS feed, an RSS autodiscovery feature is triggered. This feature does not check safety or URLs. Versions 9.5.13 and 10.0.7 contain a patch for this issue. **CVE ID : CVE-2023-28633**	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/security/advisories/GHSA-r57v-j88m-rwwf, https://github.com/glpi-project/glpi/commit/e2819da64c9075050805a44c834e1f4dc621a982	A-GLP-GLPI-200423/266
Affected Version(s): From (including) 0.85 Up to (excluding) 9.5.13					
Improper Neutralization of Input	05-Apr-2023	6.1	GLPI is a free asset and IT management software package. Starting in version	https://github.com/glpi-project/glpi/releases/tag/9.	A-GLP-GLPI-200423/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			0.85 and prior to versions 9.5.13 and 10.0.7, a malicious link can be crafted by an unauthenticated user. It will be able to exploit a reflected XSS in case any authenticated user opens the crafted link. This issue is fixed in versions 9.5.13 and 10.0.7. **CVE ID : CVE-2023-28639**	5.13, https://github.com/glpi-project/glpi/security/advisories/GHSA-r93q-chh5-jgh4, https://github.com/glpi-project/glpi/releases/tag/10.0.7	
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.7					
Improper Authorization	05-Apr-2023	8.8	GLPI is a free asset and IT management software package. Starting in version 0.83 and prior to versions 9.5.13 and 10.0.7, a user who has the Technician profile could see and generate a Personal token for a Super-Admin. Using such token it is possible to negotiate a GLPI session and hijack the Super-Admin account, resulting in a Privilege Escalation. Versions 9.5.13 and 10.0.7 contain a patch for this issue. **CVE ID : CVE-2023-28634**	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/releases/tag/10.0.7, https://github.com/glpi-project/glpi/security/advisories/GHSA-4279-rxmh-gf39	A-GLP-GLPI-200423/268
Improper Privilege	05-Apr-2023	8.1	GLPI is a free asset and IT management	https://github.com/glpi-	A-GLP-GLPI-200423/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			software package. Starting in version 0.83 and prior to versions 9.5.13 and 10.0.7, an authenticated user can modify emails of any user, and can therefore takeover another user account through the "forgotten password" feature. By modifying emails, the user can also receive sensitive data through GLPI notifications. Versions 9.5.13 and 10.0.7 contain a patch for this issue. As a workaround, account takeover can be prevented by deactivating all notifications related to `Forgotten password?` event. However, it will not prevent unauthorized modification of any user emails. **CVE ID : CVE-2023-28632**	project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/releases/tag/10.0.7, https://github.com/glpi-project/glpi/security/advisories/GHSA-7pwm-pg76-3q9x	
Improper Neutralization of Special Elements used in an SQL Command	05-Apr-2023	8.1	GLPI is a free asset and IT management software package. Starting in version 0.50 and prior to versions 9.5.13 and 10.0.7, a SQL Injection	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/s	A-GLP-GLPI-200423/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			vulnerability allow users with access rights to statistics or reports to extract all data from database and, in some cases, write a webshell on the server. Versions 9.5.13 and 10.0.7 contain a patch for this issue. As a workaround, remove `Assistance > Statistics` and `Tools > Reports` read rights from every user. **CVE ID : CVE-2023-28838**	ecurity/advisories/GHSA-2c7r-gf38-358f, https://github.com/glpi-project/glpi/releases/tag/10.0.7	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	GLPI is a free asset and IT management software package. Starting in version 0.85 and prior to versions 9.5.13 and 10.0.7, a malicious link can be crafted by an unauthenticated user. It will be able to exploit a reflected XSS in case any authenticated user opens the crafted link. This issue is fixed in versions 9.5.13 and 10.0.7. **CVE ID : CVE-2023-28639**	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/security/advisories/GHSA-r93q-chh5-jgh4, https://github.com/glpi-project/glpi/releases/tag/10.0.7	A-GLP-GLPI-200423/271
Server-Side Request	05-Apr-2023	5.4	GLPI is a free asset and IT management software package. Starting in version 0.84 and prior to	https://github.com/glpi-project/glpi/releases/tag/9.5.13,	A-GLP-GLPI-200423/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			versions 9.5.13 and 10.0.7, usage of RSS feeds is subject to server-side request forgery (SSRF). In case the remote address is not a valid RSS feed, an RSS autodiscovery feature is triggered. This feature does not check safety or URLs. Versions 9.5.13 and 10.0.7 contain a patch for this issue. **CVE ID : CVE-2023-28633**	https://github.com/glpi-project/glpi/security/advisories/GHSA-r57v-j88m-rwwf, https://github.com/glpi-project/glpi/commit/e2819da64c9075050805a44c834e1f4dc621a982	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.7, GLPI inventory endpoint can be used to drive a SQL injection attack. It can also be used to store malicious code that could be used to perform XSS attack. By default, GLPI inventory endpoint requires no authentication. Version 10.0.7 contains a patch for this issue. As a workaround, disable native inventory. **CVE ID : CVE-2023-28849**	https://github.com/glpi-project/glpi/releases/tag/10.0.7, https://github.com/glpi-project/glpi/security/advisories/GHSA-9r84-jpg3-h4m6	A-GLP-GLPI-200423/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	4.8	GLPI is a free asset and IT management software package. Starting in version 0.60 and prior to versions 9.5.13 and 10.0.7, a vulnerability allows an administrator to create a malicious external link. This issue is fixed in versions 9.5.13 and 10.0.7. **CVE ID : CVE-2023-28636**	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/releases/tag/10.0.7, https://github.com/glpi-project/glpi/security/advisories/GHSA-55pm-mc2m-pq46	A-GLP-GLPI-200423/274
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	4.8	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to versions 9.5.13 and 10.0.7, a user with dashboard administration rights may hack the dashboard form to store malicious code that will be executed when other users will use the related dashboard. Versions 9.5.13 and 10.0.7 contain a patch for this issue. **CVE ID : CVE-2023-28852**	https://github.com/glpi-project/glpi/releases/tag/9.5.13, https://github.com/glpi-project/glpi/security/advisories/GHSA-65gq-p8hg-7m92, https://github.com/glpi-project/glpi/releases/tag/10.0.7	A-GLP-GLPI-200423/275
Affected Version(s): From (including) 9.5.0 Up to (excluding) 9.5.13					
Improper Neutralization of Input	05-Apr-2023	4.8	GLPI is a free asset and IT management software package. Starting in version	https://github.com/glpi-project/glpi/releases/tag/9.	A-GLP-GLPI-200423/276

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			9.5.0 and prior to versions 9.5.13 and 10.0.7, a user with dashboard administration rights may hack the dashboard form to store malicious code that will be executed when other users will use the related dashboard. Versions 9.5.13 and 10.0.7 contain a patch for this issue. **CVE ID : CVE-2023-28852**	5.13, https://github.com/glpi-project/glpi/security/advisories/GHSA-65gq-p8hg-7m92, https://github.com/glpi-project/glpi/releases/tag/10.0.7	
Product: order					
Affected Version(s): 2.10.0					
Deserialization of Untrusted Data	05-Apr-2023	8.8	The Order GLPI plugin allows users to manage order management within GLPI. Starting with version 1.8.0 and prior to versions 2.7.7 and 2.10.1, an authenticated user that has access to standard interface can craft an URL that can be used to execute a system command. Versions 2.7.7 and 2.10.1 contain a patch for this issue. As a workaround, delete the `ajax/dropdownContact.php` file from the plugin.	https://github.com/pluginsGLPI/order/security/advisories/GHSA-xfx2-qx2r-3wwm, https://github.com/pluginsGLPI/order/commit/c78e64b95e54d5e47d9835984c93049f245b579e	A-GLP-ORDE-200423/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29006		
Affected Version(s): From (including) 1.8.0 Up to (excluding) 2.7.7					
Deserialization of Untrusted Data	05-Apr-2023	8.8	The Order GLPI plugin allows users to manage order management within GLPI. Starting with version 1.8.0 and prior to versions 2.7.7 and 2.10.1, an authenticated user that has access to standard interface can craft an URL that can be used to execute a system command. Versions 2.7.7 and 2.10.1 contain a patch for this issue. As a workaround, delete the `ajax/dropdownContact.php` file from the plugin. **CVE ID : CVE-2023-29006**	https://github.com/pluginsGLPI/order/security/advisories/GHSA-xfx2-qx2r-3wwm, https://github.com/pluginsGLPI/order/commit/c78e64b95e54d5e47d9835984c93049f245b579e	A-GLP-ORDE-200423/278
Vendor: GNU					
Product: binutils					
Affected Version(s): 2.40					
Out-of-bounds Write	03-Apr-2023	7.8	Heap based buffer overflow in binutils-gdb/bfd/libbfd.c in bfd_getl64. **CVE ID : CVE-2023-1579**	https://sourceware.org/bugzilla/show_bug.cgi?id=29988	A-GNU-BINU-200423/279
Product: screen					
Affected Version(s): * Up to (including) 4.9.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Apr-2023	7.8	socket.c in GNU Screen through 4.9.0, when installed setuid or setgid (the default on platforms such as Arch Linux and FreeBSD), allows local users to send a privileged SIGHUP signal to any PID, causing a denial of service or disruption of the target process. **CVE ID : CVE-2023-24626**	https://git.savannah.gnu.org/cgit/screen.git/patch/?id=e9ad41bfedb4537a6f0de20f00b27c7739f168f7	A-GNU-SCRE-200423/280
Vendor: go-fastdfs_project					
Product: go-fastdfs					
Affected Version(s): * Up to (including) 1.4.3					
Unrestricted Upload of File with Dangerous Type	02-Apr-2023	9.8	A vulnerability, which was classified as critical, has been found in sjqzhang go-fastdfs up to 1.4.3. Affected by this issue is the function upload of the file /group1/uploa of the component File Upload Handler. The manipulation leads to path traversal: '../filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224768. **CVE ID : CVE-2023-1800**	N/A	A-GO--GO-F-200423/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.19.8					
Improper Control of Generation of Code ('Code Injection')	06-Apr-2023	9.8	Templates do not properly consider backticks (`) as Javascript string delimiters, and do not escape them as expected. Backticks are used, since ES6, for JS template literals. If a template contains a Go template action within a Javascript template literal, the contents of the action can be used to terminate the literal, injecting arbitrary Javascript code into the Go template. As ES6 template literals are rather complex, and themselves can do string interpolation, the decision was made to simply disallow Go template actions from being used inside of them (e.g. "var a = {{.}}"), since there is no obviously safe way to allow this behavior. This takes the same approach as github.com/google/safehtml. With fix, Template.Parse returns an Error	https://go.dev/cl/482079, https://pkg.go.dev/vuln/GO-2023-1703, https://go.dev/issue/59234	A-GOL-GO-200423/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when it encounters templates like this, with an ErrorCode of value 12. This ErrorCode is currently unexported, but will be exported in the release of Go 1.21. Users who rely on the previous behavior can re-enable it using the GODEBUG flag jstmpllitinterp=1, with the caveat that backticks will now be escaped. This should be used with caution. **CVE ID : CVE-2023-24538**		
Allocation of Resources Without Limits or Throttling	06-Apr-2023	7.5	Multipart form parsing can consume large amounts of CPU and memory when processing form inputs containing very large numbers of parts. This stems from several causes: 1. mime/multipart.Reader.ReadForm limits the total memory a parsed multipart form can consume. ReadForm can undercount the amount of memory consumed, leading it to accept larger inputs than intended.	https://go.dev/cl/482077, https://go.dev/cl/482076, https://go.dev/cl/482075, https://go.dev/issue/59153, https://pkg.go.dev/vuln/GO-2023-1705	A-GOL-GO-200423/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2. Limiting total memory does not account for increased pressure on the garbage collector from large numbers of small allocations in forms with many parts. 3. ReadForm can allocate a large number of short-lived buffers, further increasing pressure on the garbage collector. The combination of these factors can permit an attacker to cause an program that parses multipart forms to consume large amounts of CPU and memory, potentially resulting in a denial of service. This affects programs that use mime/multipart.Reader.ReadForm, as well as form parsing in the net/http package with the Request methods FormFile, FormValue, ParseMultipartForm, and PostFormValue. With fix, ReadForm now does a better job of estimating the memory consumption of parsed forms, and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performs many fewer short-lived allocations. In addition, the fixed mime/multipart.Reader imposes the following limits on the size of parsed forms: 1. Forms parsed with ReadForm may contain no more than 1000 parts. This limit may be adjusted with the environment variable GODEBUG=multipartmaxparts=. 2. Form parts parsed with NextPart and NextRawPart may contain no more than 10,000 header fields. In addition, forms parsed with ReadForm may contain no more than 10,000 header fields across all parts. This limit may be adjusted with the environment variable GODEBUG=multipartmaxheaders=. **CVE ID : CVE-2023-24536**		
Integer Overflow or Wraparound	06-Apr-2023	7.5	Calling any of the Parse functions on Go source code which contains //line directives	https://go.dev/cl/482078, https://go.dev/issue/59180, https://group	A-GOL-GO-200423/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with very large line numbers can cause an infinite loop due to integer overflow. **CVE ID : CVE-2023-24537**	s.google.com/g/golang-announce/c/Xdv6JL9ENs8, https://pkg.go.dev/vuln/GO-2023-1702	
Affected Version(s): From (including) 1.20.0 Up to (excluding) 1.20.3					
Improper Control of Generation of Code ('Code Injection')	06-Apr-2023	9.8	Templates do not properly consider backticks (`) as Javascript string delimiters, and do not escape them as expected. Backticks are used, since ES6, for JS template literals. If a template contains a Go template action within a Javascript template literal, the contents of the action can be used to terminate the literal, injecting arbitrary Javascript code into the Go template. As ES6 template literals are rather complex, and themselves can do string interpolation, the decision was made to simply disallow Go template actions from being used inside of them (e.g. "var a = {{.}}"), since there is no obviously safe way to allow this behavior. This takes the same	https://go.dev/cl/482079, https://pkg.go.dev/vuln/GO-2023-1703, https://go.dev/issue/59234	A-GOL-GO-200423/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			approach as github.com/google/safehtml. With fix, Template.Parse returns an Error when it encounters templates like this, with an ErrorCode of value 12. This ErrorCode is currently unexported, but will be exported in the release of Go 1.21. Users who rely on the previous behavior can re-enable it using the GODEBUG flag jstmpllitinterp=1, with the caveat that backticks will now be escaped. This should be used with caution. **CVE ID : CVE-2023-24538**		
Allocation of Resources Without Limits or Throttling	06-Apr-2023	7.5	Multipart form parsing can consume large amounts of CPU and memory when processing form inputs containing very large numbers of parts. This stems from several causes: 1. mime/multipart.Reader.ReadForm limits the total memory a parsed multipart form can consume. ReadForm can	https://go.dev/cl/482077, https://go.dev/cl/482076, https://go.dev/cl/482075, https://go.dev/issue/59153, https://pkg.go.dev/vuln/GO-2023-1705	A-GOL-GO-200423/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undercount the amount of memory consumed, leading it to accept larger inputs than intended. 2. Limiting total memory does not account for increased pressure on the garbage collector from large numbers of small allocations in forms with many parts. 3. ReadForm can allocate a large number of short-lived buffers, further increasing pressure on the garbage collector. The combination of these factors can permit an attacker to cause an program that parses multipart forms to consume large amounts of CPU and memory, potentially resulting in a denial of service. This affects programs that use mime/multipart.Reader.ReadForm, as well as form parsing in the net/http package with the Request methods FormFile, FormValue, ParseMultipartForm, and PostFormValue. With fix, ReadForm		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			now does a better job of estimating the memory consumption of parsed forms, and performs many fewer short-lived allocations. In addition, the fixed mime/multipart.Reader imposes the following limits on the size of parsed forms: 1. Forms parsed with ReadForm may contain no more than 1000 parts. This limit may be adjusted with the environment variable GODEBUG=multipartmaxparts=. 2. Form parts parsed with NextPart and NextRawPart may contain no more than 10,000 header fields. In addition, forms parsed with ReadForm may contain no more than 10,000 header fields across all parts. This limit may be adjusted with the environment variable GODEBUG=multipartmaxheaders=. **CVE ID : CVE-2023-24536**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	7.5	Calling any of the Parse functions on Go source code which contains //line directives with very large line numbers can cause an infinite loop due to integer overflow. **CVE ID : CVE-2023-24537**	https://go.dev/cl/482078, https://go.dev/issue/59180, https://groups.google.com/g/golang-announce/c/Xdv6JL9ENs8, https://pkg.go.dev/vuln/GO-2023-1702	A-GOL-GO-200423/287
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 112.0.5615.49					
Out-of-bounds Write	04-Apr-2023	8.8	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 crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1810**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/288
Use After Free	04-Apr-2023	8.8	Use after free in Frames 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.	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(Chromium security severity: High) **CVE ID : CVE-2023-1811**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Apr-2023	8.8	Out of bounds memory access in DOM Bindings in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1812**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/290
Use After Free	04-Apr-2023	8.8	Use after free in Networking APIs 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: Medium) **CVE ID : CVE-2023-1815**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/291
Use After Free	04-Apr-2023	8.8	Use after free in Vulkan in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1818**		
Out-of-bounds Write	04-Apr-2023	8.8	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: Medium) **CVE ID : CVE-2023-1820**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/293
N/A	04-Apr-2023	6.5	Inappropriate implementation in Extensions in Google Chrome prior to 112.0.5615.49 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1813**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/294
Improper Input Validation	04-Apr-2023	6.5	Insufficient validation of untrusted input in Safe Browsing in	https://chromereleases.googleblog.com/2023/04/stable-	A-GOO-CHRO-200423/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass download checking via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1814**	channel-update-for-desktop.html	
N/A	04-Apr-2023	6.5	Incorrect security UI in Picture In Picture in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially perform navigation spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1816**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/296
N/A	04-Apr-2023	6.5	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 security severity: Medium) **CVE ID : CVE-2023-1817**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Apr-2023	6.5	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 security severity: Medium) **CVE ID : CVE-2023-1819**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/298
N/A	04-Apr-2023	6.5	Inappropriate implementation in WebShare in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1821**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/299
N/A	04-Apr-2023	6.5	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: Low) **CVE ID : CVE-2023-1822**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Apr-2023	6.5	Inappropriate implementation in FedCM in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1823**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	A-GOO-CHRO-200423/301
Vendor: goprayer					
Product: wp_prayer					
Affected Version(s): * Up to (excluding) 1.9.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Go Prayer WP Prayer plugin <= 1.9.6 versions. **CVE ID : CVE-2023-25705**	N/A	A-GOP-WP_P-200423/302
Vendor: groundhogg					
Product: groundhogg					
Affected Version(s): * Up to (excluding) 2.7.9.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Apr-2023	7.2	The WordPress CRM, Email & Marketing Automation for WordPress | Award Winner — Groundhogg WordPress plugin before 2.7.9.4 does not properly sanitise and escape a parameter before using it in a SQL	N/A	A-GRO-GROU-200423/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			statement, leading to a SQL injection exploitable by high privilege users such as admins **CVE ID : CVE-2023-1425**		
Vendor: hashicorp					
Product: nomad					
Affected Version(s): From (including) 1.5.0 Up to (including) 1.5.2					
Missing Authorization	05-Apr-2023	9.8	HashiCorp Nomad and Nomad Enterprise versions 1.5.0 up to 1.5.2 allow unauthenticated users to bypass intended ACL authorizations for clusters where mTLS is not enabled. This issue is fixed in version 1.5.3. **CVE ID : CVE-2023-1782**	https://discuss.hashicorp.com/t/hcsec-2023-12-nomad-unauthenticated-client-agent-http-request-privilege-escalation/52375	A-HAS-NOMA-200423/304
Vendor: hasthemes					
Product: really_simple_google_tag_manager					
Affected Version(s): * Up to (excluding) 1.0.7					
Cross-Site Request Forgery (CSRF)	06-Apr-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes Really Simple Google Tag Manager plugin <= 1.0.6 versions. **CVE ID : CVE-2023-23801**	N/A	A-HAS-REAL-200423/305
Vendor: heateor					
Product: social_comments					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Team Heateor WordPress Social Comments Plugin for Vkontakte Comments and Disqus Comments plugin <= 1.6.1 versions. **CVE ID : CVE-2023-23977**	N/A	A-HEA-SOCI-200423/306
Vendor: helpy.io					
Product: helpy					
Affected Version(s): 2.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	6.1	Helpy version 2.8.0 allows an unauthenticated remote attacker to exploit an XSS stored in the application. This is possible because the application does not correctly validate the attachments sent by customers in the ticket. **CVE ID : CVE-2023-0357**	N/A	A-HEL-HELP-200423/307
Vendor: htmlunit_project					
Product: htmlunit					
Affected Version(s): * Up to (excluding) 3.0.0					
N/A	03-Apr-2023	9.8	Versions of the package net.sourceforge.htmlunit:htmlunit from 0	https://github.com/HtmlUnit/htmlunit/commit/641325	A-HTM-HTML-200423/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and before 3.0.0 are vulnerable to Remote Code Execution (RCE) via XSTL, when browsing the attacker’s webpage. **CVE ID : CVE-2023-26119**	bbc84702dc9800ec7037aec061ce21956b	
Vendor: i13websolution					
Product: continuous_image_carosel_with_lightbox					
Affected Version(s): * Up to (excluding) 1.0.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Continuous Image Carousel With Lightbox plugin <= 1.0.15 versions. **CVE ID : CVE-2023-28792**	N/A	A-I13-CONT-200423/309
Vendor: ibenic					
Product: simple_giveaways					
Affected Version(s): * Up to (excluding) 2.45.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The Simple Giveaways WordPress plugin before 2.45.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for	N/A	A-IBE-SIMP-200423/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example in multisite setup) **CVE ID : CVE-2023-1120**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The Simple Giveaways WordPress plugin before 2.45.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-1121**	N/A	A-IBE-SIMP-200423/311
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The Simple Giveaways WordPress plugin before 2.45.1 does not sanitise and escape some of its Giveaways options, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	A-IBE-SIMP-200423/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1122		
Vendor: IBM					
Product: aspera_cargo					
Affected Version(s): * Up to (excluding) 4.2.5					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Apr-2023	9.8	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616. **CVE ID : CVE-2023-27284**	https://www.ibm.com/support/pages/node/6966588	A-IBM-ASPE-200423/313
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Apr-2023	9.8	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616. **CVE ID : CVE-2023-27286**	https://www.ibm.com/support/pages/node/6966588, https://exchange.xforce.ibmcloud.com/vulnerabilities/248627	A-IBM-ASPE-200423/314
Product: aspera_connect					
Affected Version(s): * Up to (excluding) 4.2.5					
Improper Restriction of Operations	02-Apr-2023	9.8	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a	https://www.ibm.com/supp	A-IBM-ASPE-200423/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616. **CVE ID : CVE-2023-27284**	ort/pages/node/6966588	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Apr-2023	9.8	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616. **CVE ID : CVE-2023-27286**	https://www.ibm.com/support/pages/node/6966588, https://exchange.xforce.ibmcloud.com/vulnerabilities/248627	A-IBM-ASPE-200423/316
Product: tririga_application_platform					
Affected Version(s): 4.0					
Improper Restriction of XML External Entity Reference	07-Apr-2023	7.1	IBM TRIRIGA 4.0 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 249975.	https://exchange.xforce.ibmcloud.com/vulnerabilities/249975, https://www.ibm.com/support/pages/node/6981115	A-IBM-TRIR-200423/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27876		
Product: websphere_application_server					
Affected Version(s): 9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 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 trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248416, https://www.ibm.com/support/pages/node/6964836	A-IBM-WEBS-200423/318
Vendor: icegram					
Product: icegram_collect					
Affected Version(s): * Up to (including) 1.3.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Icegram Icegram Collect plugin <= 1.3.8 versions. **CVE ID : CVE-2023-25024**	N/A	A-ICE-ICEG-200423/319
Vendor: image_over_image_for_wpbakery_page_builder_project					
Product: image_over_image_for_wpbakery_page_builder					
Affected Version(s): * Up to (excluding) 3.0					
Improper Neutralizat	03-Apr-2023	5.4	The Image Over Image For WPBakery	N/A	A-IMA-IMAG-200423/320

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Page Builder WordPress plugin before 3.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0399**		
Vendor: imaworldhealth					
Product: bhima					
Affected Version(s): 1.27.0					
Improper Privilege Management	05-Apr-2023	6.5	Bhima version 1.27.0 allows a remote attacker to update the privileges of any account registered in the application via a malicious link sent to an administrator. This is possible because the application is vulnerable to CSRF. **CVE ID : CVE-2023-0959**	N/A	A-IMA-BHIM-200423/321
Authorization Bypass Through User-Controlled Key	05-Apr-2023	6.5	Bhima version 1.27.0 allows an attacker authenticated with normal user permissions to view sensitive data of other application	N/A	A-IMA-BHIM-200423/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users and data that should only be viewed by the administrator. This is possible because the application is vulnerable to IDOR, it does not properly validate user permissions with respect to certain actions the user can perform. **CVE ID : CVE-2023-0967**		
Incorrect Permission Assignment for Critical Resource	05-Apr-2023	4.3	Bhima version 1.27.0 allows an authenticated attacker with regular user permissions to update arbitrary user session data such as username, email and password. This is possible because the application is vulnerable to IDOR, it does not correctly validate user permissions with respect to certain actions that can be performed by the user. **CVE ID : CVE-2023-0944**	N/A	A-IMA-BHIM-200423/323
Vendor: implecode					
Product: ecommerce_product_catalog					
Affected Version(s): * Up to (including) 3.3.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in impleCode eCommerce Product Catalog Plugin for WordPress plugin <= 3.3.4 versions. **CVE ID : CVE-2023-25049**	N/A	A-IMP-ECOM-200423/324
Product: product_catalog_simple					
Affected Version(s): * Up to (excluding) 1.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in impleCode Product Catalog Simple plugin <= 1.6.17 versions. **CVE ID : CVE-2023-29388**	N/A	A-IMP-PROD-200423/325
Vendor: incsub					
Product: hummingbird					
Affected Version(s): * Up to (excluding) 3.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Apr-2023	9.8	The Hummingbird WordPress plugin before 3.4.2 does not validate the generated file path for page cache files before writing them, leading to a path traversal vulnerability in the page cache module. **CVE ID : CVE-2023-1478**	N/A	A-INC-HUMM-200423/326
Vendor: inisev					
Product: redirection					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.1.4					
Cross-Site Request Forgery (CSRF)	03-Apr-2023	6.5	The Redirection WordPress plugin before 1.1.4 does not add nonce verification in place when adding the redirect, which could allow attackers to add redirects via a CSRF attack. **CVE ID : CVE-2023-1330**	N/A	A-INI-REDI-200423/327
Vendor: interactive_polish_map_project					
Product: interactive_polish_map					
Affected Version(s): * Up to (excluding) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marcin Pietrzak Interactive Polish Map plugin <= 1.2 versions. **CVE ID : CVE-2023-23821**	N/A	A-INT-INTE-200423/328
Vendor: intranda					
Product: goobi_viewer_core					
Affected Version(s): * Up to (excluding) 23.03					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	6.1	The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. A reflected cross-site scripting vulnerability has been identified in Goobi viewer core prior to version	https://github.com/intranda/goobi-viewer-core/security/advisories/GHSA-7v7g-9vx6-vcg2, https://github.com/intranda/goobi-	A-INT-GOOB-200423/329

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23.03 when evaluating the LOGID parameter. An attacker could trick a user into following a specially crafted link to a Goobi viewer installation, resulting in the execution of malicious script code in the user's browser. The vulnerability has been fixed in version 23.03. **CVE ID : CVE-2023-29014**	viewer-core/commit/c29efe60e745a94d03debc17681c4950f3917455	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	6.1	The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. A cross-site scripting vulnerability has been identified in the user comment feature of Goobi viewer core prior to version 23.03. An attacker could create a specially crafted comment, resulting in the execution of malicious script code in the user's browser when displaying the comment. The vulnerability has been fixed in version 23.03. **CVE ID : CVE-2023-29015**	https://github.com/intranda/goobi-viewer-core/commit/f0ccde2d469efd9597c3062d00177a63341f2256, https://github.com/intranda/goobi-viewer-core/security/advisories/GHSA-622w-995c-3c3h	A-INT-GOOB-200423/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	6.1	The Goobi viewer is a web application that allows digitised material to be displayed in a web browser. A cross-site scripting vulnerability has been identified in Goobi viewer core prior to version 23.03 when using nicknames. An attacker could create a user account and enter malicious scripts into their profile's nickname, resulting in the execution in the user's browser when displaying the nickname on certain pages. The vulnerability has been fixed in version 23.03. **CVE ID : CVE-2023-29016**	https://github.com/intranda/goobi-viewer-core/commit/8eadb32b3fdcb775678b74d95bc3df018a5d5238, https://github.com/intranda/goobi-viewer-core/security/advisories/GHSA-2r9r-8fcg-m38g	A-INT-GOOB-200423/331
Vendor: Irfanview					
Product: irfanview					
Affected Version(s): 4.62					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Apr-2023	5.5	Irfanview v4.62 allows a user-mode write access violation via a crafted JPEG 2000 file starting at JPEG2000+0x0000000000001bf0. **CVE ID : CVE-2023-26974**	N/A	A-IRF-IRFA-200423/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: javadelight					
Product: nashorn_sandbox					
Affected Version(s): 0.2.4					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-Apr-2023	7.2	delight-nashorn-sandbox 0.2.4 and 0.2.5 is vulnerable to sandbox escape. When allowExitFunctions is set to false, the loadWithNewGlobal function can be used to invoke the exit and quit methods to exit the Java process. **CVE ID : CVE-2023-26919**	https://github.com/javadelight/delight-nashorn-sandbox/issues/135	A-JAV-NASH-200423/333
Affected Version(s): 0.2.5					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-Apr-2023	7.2	delight-nashorn-sandbox 0.2.4 and 0.2.5 is vulnerable to sandbox escape. When allowExitFunctions is set to false, the loadWithNewGlobal function can be used to invoke the exit and quit methods to exit the Java process. **CVE ID : CVE-2023-26919**	https://github.com/javadelight/delight-nashorn-sandbox/issues/135	A-JAV-NASH-200423/334
Vendor: Jenkins					
Product: convert_to_pipeline					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Special Elements	02-Apr-2023	9.8	Jenkins Convert To Pipeline Plugin 1.0 and earlier uses basic string concatenation to	https://www.jenkins.io/security/advisory/2023-03-	A-JEN-CONV-200423/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			convert Freestyle projects' Build Environment, Build Steps, and Post-build Actions to the equivalent Pipeline step invocations, allowing attackers able to configure Freestyle projects to prepare a crafted configuration that injects Pipeline script code into the (unsandboxed) Pipeline resulting from a convertion by Jenkins Convert To Pipeline Plugin. **CVE ID : CVE-2023-28677**	21/#SECURITY-2966	
Cross-Site Request Forgery (CSRF)	02-Apr-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins Convert To Pipeline Plugin 1.0 and earlier allows attackers to create a Pipeline based on a Freestyle project, potentially leading to remote code execution (RCE). **CVE ID : CVE-2023-28676**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2963	A-JEN-CONV-200423/336
Product: cppcheck					
Affected Version(s): * Up to (including) 1.26					
Improper Neutralization of Input During	02-Apr-2023	5.4	Jenkins Cppcheck Plugin 1.26 and earlier does not escape file names from Cppcheck	https://www.jenkins.io/security/advisory/2023-03-	A-JEN-CPPC-200423/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			report files before showing them on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control report file contents. **CVE ID : CVE-2023-28678**	21/#SECURITY-2809	
Product: crap4j					
Affected Version(s): * Up to (including) 0.9					
Improper Restriction of XML External Entity Reference	02-Apr-2023	7.5	Jenkins Crap4J Plugin 0.9 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2023-28680**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2925	A-JEN-CRAP-200423/338
Product: jacoco					
Affected Version(s): * Up to (including) 3.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	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 action.	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-3061	A-JEN-JACO-200423/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28669		
Product: mashup_portlets					
Affected Version(s): * Up to (including) 1.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	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-site scripting (XSS) vulnerability exploitable by authenticated attackers with Overall/Read permission. **CVE ID : CVE-2023-28679**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2813	A-JEN-MASH-200423/340
Product: octoperf_load_testing					
Affected Version(s): * Up to (including) 4.5.0					
Cross-Site Request Forgery (CSRF)	02-Apr-2023	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-3067%20(1)	A-JEN-OCTO-200423/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28671		
Affected Version(s): * Up to (including) 4.5.1					
Missing Authorization	02-Apr-2023	6.5	Jenkins OctoPerf Load Testing Plugin Plugin 4.5.1 and earlier does not perform a permission check in a connection test HTTP endpoint, allowing attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2023-28672**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-3067%20(2)	A-JEN-OCTO-200423/342
Affected Version(s): * Up to (including) 4.5.2					
Cross-Site Request Forgery (CSRF)	02-Apr-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers to connect to a previously configured Octoperf server using attacker-specified credentials. **CVE ID : CVE-2023-28674**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-3067%20(4)	A-JEN-OCTO-200423/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	02-Apr-2023	4.3	A missing permission check in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2023-28673**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-3067%20(3)	A-JEN-OCTO-200423/344
Missing Authorization	02-Apr-2023	4.3	A missing permission check in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers to connect to a previously configured Octoperf server using attacker-specified credentials. **CVE ID : CVE-2023-28675**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-3067%20(4)	A-JEN-OCTO-200423/345
Product: performance_publisher					
Affected Version(s): * Up to (including) 8.09					
Improper Restriction of XML External Entity Reference	02-Apr-2023	8.2	Jenkins Performance Publisher Plugin 8.09 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2023-28682**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2928	A-JEN-PERF-200423/346
Product: phabricator_differential					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.1.5					
Improper Restriction of XML External Entity Reference	02-Apr-2023	8.2	Jenkins Phabricator Differential Plugin 2.1.5 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2023-28683**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2942	A-JEN-PHAB-200423/347
Product: pipeline_aggregator_view					
Affected Version(s): * Up to (including) 1.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	Jenkins Pipeline Aggregator View Plugin 1.13 and earlier does not escape a variable representing the current view's URL in inline JavaScript, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by authenticated attackers with Overall/Read permission. **CVE ID : CVE-2023-28670**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2885	A-JEN-PIPE-200423/348
Product: remote-jobs-view					
Affected Version(s): * Up to (including) 0.0.3					
Improper Restriction of XML External Entity Reference	02-Apr-2023	6.5	Jenkins remote-jobs-view-plugin Plugin 0.0.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2956	A-JEN-REMO-200423/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28684		
Product: role-based_authorization_strategy					
Affected Version(s): * Up to (including) 587.v2872c41fa_e51					
Improper Preservation of Permissions	02-Apr-2023	9.8	Jenkins Role-based Authorization Strategy Plugin 587.v2872c41fa_e51 and earlier grants permissions even after they've been disabled. **CVE ID : CVE-2023-28668**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-3053	A-JEN-ROLE-200423/350
Product: visual_studio_code_metrics					
Affected Version(s): * Up to (including) 1.7					
Improper Restriction of XML External Entity Reference	02-Apr-2023	8.2	Jenkins Visual Studio Code Metrics Plugin 1.7 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2023-28681**	https://www.jenkins.io/security/advisory/2023-03-21/#SECURITY-2926	A-JEN-VISU-200423/351
Vendor: jflyfox					
Product: jfinal_cms					
Affected Version(s): 5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Jfinal CMS v5.1 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /system/dict/list. **CVE ID : CVE-2023-24747**	N/A	A-JFL-JFIN-200423/352
Vendor: joinmastodon					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mastodon					
Affected Version(s): From (including) 2.5.0 Up to (excluding) 3.5.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Apr-2023	6.5	Mastodon is a free, open-source social network server based on ActivityPub Mastodon allows configuration of LDAP for authentication. Starting in version 2.5.0 and prior to versions 3.5.8, 4.0.4, and 4.1.2, the LDAP query made during login is insecure and the attacker can perform LDAP injection attack to leak arbitrary attributes from LDAP database. This issue is fixed in versions 3.5.8, 4.0.4, and 4.1.2. **CVE ID : CVE-2023-28853**	https://github.com/mastodon/mastodon/security/advisories/GHSA-38g9-pfm9-gfqv, https://github.com/mastodon/mastodon/pull/24379	A-JOI-MAST-200423/353
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.4					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Apr-2023	6.5	Mastodon is a free, open-source social network server based on ActivityPub Mastodon allows configuration of LDAP for authentication. Starting in version 2.5.0 and prior to versions 3.5.8, 4.0.4, and 4.1.2, the LDAP query made during login is insecure and the attacker can	https://github.com/mastodon/mastodon/security/advisories/GHSA-38g9-pfm9-gfqv, https://github.com/mastodon/mastodon/pull/24379	A-JOI-MAST-200423/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform LDAP injection attack to leak arbitrary attributes from LDAP database. This issue is fixed in versions 3.5.8, 4.0.4, and 4.1.2. **CVE ID : CVE-2023-28853**		
Affected Version(s): From (including) 4.1.0 Up to (excluding) 4.1.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Apr-2023	6.5	Mastodon is a free, open-source social network server based on ActivityPub Mastodon allows configuration of LDAP for authentication. Starting in version 2.5.0 and prior to versions 3.5.8, 4.0.4, and 4.1.2, the LDAP query made during login is insecure and the attacker can perform LDAP injection attack to leak arbitrary attributes from LDAP database. This issue is fixed in versions 3.5.8, 4.0.4, and 4.1.2. **CVE ID : CVE-2023-28853**	https://github.com/mastodon/mastodon/security/advisories/GHSA-38g9-pfm9-gfqv, https://github.com/mastodon/mastodon/pull/24379	A-JOI-MAST-200423/355
Vendor: joomunited					
Product: wp_meta_seo					
Affected Version(s): * Up to (excluding) 4.5.5					
Deserialization of Untrusted Data	10-Apr-2023	8.8	The WP Meta SEO WordPress plugin before 4.5.5 does not validate image file	N/A	A-JOO-WP_M-200423/356

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			paths before attempting to manipulate the image files, leading to a PHAR deserialization vulnerability. Furthermore, the plugin contains a gadget chain which may be used in certain configurations to achieve remote code execution. **CVE ID : CVE-2023-1381**		
Vendor: keetrax					
Product: wp_tiles					
Affected Version(s): * Up to (including) 1.1.2					
N/A	10-Apr-2023	6.5	The WP Tiles WordPress plugin through 1.1.2 does not ensure that posts to be displayed are not draft/private, allowing any authenticated users, such as subscriber to retrieve the titles of draft and privates posts for example. AN attacker could also retrieve the title of any other type of post. **CVE ID : CVE-2023-1426**	N/A	A-KEE-WP_T-200423/357
Vendor: keysight					
Product: hawkeye					
Affected Version(s): 3.3.16.28					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	A vulnerability was found in Keysight IXIA Hawkeye 3.3.16.28. It has been declared as problematic. This vulnerability affects unknown code of the file /licenses. The manipulation of the argument view with the input teste"><script>alert(%27c4ng4c3ir0%27)</script> leads to cross site scripting. The attack can be initiated remotely. VDB-224998 is the identifier assigned to this vulnerability. NOTE: Vendor did not respond if and how they may handle this issue. **CVE ID : CVE-2023-1860**	N/A	A-KEY-HAWK-200423/358
Vendor: Kibokolabs					
Product: arigato_autoresponder_and_newsletter					
Affected Version(s): * Up to (including) 2.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter plugin <= 2.7.1 versions. **CVE ID : CVE-2023-25031**	N/A	A-KIB-ARIG-200423/359
Affected Version(s): * Up to (including) 2.7.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter plugin <= 2.7.1.1 versions. **CVE ID : CVE-2023-25020**	N/A	A-KIB-ARIG-200423/360
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Arigato Autoresponder and Newsletter plugin <= 2.7.1.1 versions. **CVE ID : CVE-2023-25061**	N/A	A-KIB-ARIG-200423/361
Product: chained_quiz					
Affected Version(s): * Up to (including) 1.3.2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Chained Quiz plugin <= 1.3.2.5 versions. **CVE ID : CVE-2023-25027**	N/A	A-KIB-CHAI-200423/362
Product: namaste\!_lms					
Affected Version(s): * Up to (excluding) 2.5.9.2					
Improper Neutralization of Input During Web Page Generation	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Namaste! LMS plugin <= 2.5.9.1 versions.	N/A	A-KIB-NAMA-200423/363

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-24383**		
Product: watu_quiz					
Affected Version(s): * Up to (including) 3.3.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kiboko Labs Watu Quiz plugin <= 3.3.8 versions. **CVE ID : CVE-2023-25022**	N/A	A-KIB-WATU-200423/364
Vendor: klaviyo					
Product: klavio					
Affected Version(s): * Up to (excluding) 3.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The Klaviyo WordPress plugin before 3.0.10 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2023-0874**	N/A	A-KLA-KLAV-200423/365
Vendor: langchain					
Product: langchain					
Affected Version(s): * Up to (including) 0.0.131					
Improper Neutralizat	05-Apr-2023	9.8	In LangChain through 0.0.131, the	https://github.com/hwchase	A-LAN-LANG-200423/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements in Output Used by a Downstream Component ('Injection')			LLMMathChain chain allows prompt injection attacks that can execute arbitrary code via the Python exec method. **CVE ID : CVE-2023-29374**	17/langchain/pull/1119, https://github.com/hwchase17/langchain/issues/814	
Vendor: limit_login_attempts_project					
Product: limit_login_attempts					
Affected Version(s): * Up to (including) 1.7.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	6.1	The Limit Login Attempts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its lock logging feature in versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the plugin's settings page. This only works when the plugin prioritizes use of the X-FORWARDED-FOR header, which can be configured in its settings.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=551920%40limit-login-attempts%2Ftags%2F1.7.1&new=2893850%40limit-login-attempts%2Ftags%2F1.7.2	A-LIM-LIMI-200423/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1912		
Vendor: linksoftwarellc					
Product: wp_terms_popup					
Affected Version(s): * Up to (excluding) 2.6.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Link Software LLC WP Terms Popup plugin <= 2.6.0 versions. **CVE ID : CVE-2023-24006**	N/A	A-LIN-WP_T-200423/368
Vendor: liveaction					
Product: livesp					
Affected Version(s): 21.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	A cross-site scripting (XSS) vulnerability in LiveAction LiveSP v21.1.2 allows attackers to execute arbitrary web scripts or HTML. **CVE ID : CVE-2023-24721**	N/A	A-LIV-LIVE-200423/369
Vendor: m-files					
Product: m-files_server					
Affected Version(s): * Up to (excluding) 23.4.12528.1					
Uncontrolled Resource Consumption	05-Apr-2023	6.5	User-controlled operations could have allowed Denial of Service in M-Files Server before 23.4.12528.1 due to uncontrolled memory consumption.	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-0382/	A-M-F-M-FI-200423/370

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0382		
Vendor: magic-post-thumbnail					
Product: magic_post_thumbnail					
Affected Version(s): * Up to (excluding) 4.1.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-site Scripting (XSS) vulnerability in Magic Post Thumbnail plugin <= 4.1.10 versions. **CVE ID : CVE-2023-29171**	N/A	A-MAG-MAGI-200423/371
Vendor: mailoptin					
Product: mailoptin					
Affected Version(s): * Up to (excluding) 1.2.54.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in MailOptin Popup Builder Team MailOptin plugin <= 1.2.54.0 versions. **CVE ID : CVE-2023-23980**	N/A	A-MAI-MAIL-200423/372
Vendor: markdown-pdf_project					
Product: markdown-pdf					
Affected Version(s): 11.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	8.2	markdown-pdf version 11.0.0 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate the	N/A	A-MAR-MARK-200423/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Markdown content entered by the user. **CVE ID : CVE-2023-0835**		
Vendor: material_design_icons_for_page_builders_project					
Product: material_design_icons_for_page_builders					
Affected Version(s): * Up to (excluding) 1.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Photon WP Material Design Icons for Page Builders plugin <= 1.4.2 versions. **CVE ID : CVE-2023-24374**	N/A	A-MAT-MATE-200423/374
Vendor: Microsoft					
Product: 365_apps					
Affected Version(s): -					
N/A	11-Apr-2023	7.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-28285**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28285	A-MIC-365_-200423/375
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 112.0.5615.49					
URL Redirection to Untrusted Site ('Open Redirect')	11-Apr-2023	6.1	Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID : CVE-2023-24935**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24935	A-MIC-EDGE-200423/376
Product: office					
Affected Version(s): 2019					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-28285**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28285	A-MIC-OFFI-200423/377
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	11-Apr-2023	7.8	Microsoft Office Remote Code Execution Vulnerability **CVE ID : CVE-2023-28285**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28285	A-MIC-OFFI-200423/378
Product: visual_studio_code					
Affected Version(s): * Up to (excluding) 1.77.0					
N/A	11-Apr-2023	7.8	Visual Studio Code Remote Code Execution Vulnerability **CVE ID : CVE-2023-24893**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24893	A-MIC-VISU-200423/379
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 1.3.3					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	9.8	Command Injection in GitHub repository microweber/microweber prior to 1.3.3. **CVE ID : CVE-2023-1877**	https://huntr.dev/bounties/71fe4b3b-20ac-448c-8191-7b99d7ffaf55, https://github.com/microweber/microweber/commit/93a906d0bf096c3ab1674012a90c88d101e76c8d	A-MIC-MICR-200423/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.3. **CVE ID : CVE-2023-1881**	https://huntr.dev/bounties/d5ebc2bd-8638-41c4-bf72-7c906c601344, https://github.com/microweber/microweber/commit/8d039de2d615956f6df8df0bb1045ff3be88f183	A-MIC-MICR-200423/381
Vendor: mobyproject					
Product: moby					
Affected Version(s): From (including) 1.12.0 Up to (excluding) 20.10.24					
Observable Discrepancy	04-Apr-2023	8.7	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon component (`dockerd`), which is developed as moby/moby, is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in dockerd and is thus present in most major Moby downstreams, is a	https://github.com/moby/libnetwork/security/advisories/GHSA-gvm4-2qqg-m333, https://github.com/moby/moby/security/advisories/GHSA-232p-vwff-86mp, https://github.com/moby/moby/security/advisories/GHSA-vwm3-crmr-xfxw, https://github.com/moby/moby/pull/45118	A-MOB-MOBY-200423/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The overlay network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with a VXLAN Network ID (VNI) that identifies the originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both incoming and outgoing IPSec. These rules rely on the u32 iptables extension provided by the xt_u32 kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	other overlay networks or other users of VXLAN. Two iptables rules serve to filter incoming VXLAN datagrams with a VNI that corresponds to an encrypted network and discards unencrypted datagrams. The rules are appended to the end of the INPUT filter chain, following any rules that have been previously set by the system administrator. Administrator-set rules take precedence over the rules Moby sets to discard unencrypted VXLAN datagrams, which can potentially admit unencrypted datagrams that should have been discarded. The injection of arbitrary Ethernet frames can enable a Denial of Service attack. A sophisticated attacker may be able to establish a UDP or TCP connection by way of the container’s outbound gateway that would otherwise be blocked by a stateful firewall,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or carry out other escalations beyond simple injection by smuggling packets into the overlay network. Patches are available in Moby releases 23.0.3 and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. Close the VXLAN port (by default, UDP port 4789) to incoming traffic at the Internet boundary to prevent all VXLAN packet injection, and/or ensure that the `xt_u32` kernel module is available on all nodes of the Swarm cluster. **CVE ID : CVE-2023-28840**		
Missing Encryption of Sensitive Data	04-Apr-2023	6.8	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon	https://github.com/moby/libnetwork/security/advisories/GHSA-gvm4-2qqg-m333, https://github.com/moby/moby/security/advisories/GHSA-vwm3-	A-MOB-MOBY-200423/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component (`dockerd`), which is developed as moby/moby is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in `dockerd` and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The `overlay` network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with the VXLAN metadata, including a VXLAN Network ID (VNI) that identifies the	crmr-xfxw, https://github.com/moby/moby/security/advisories/GHSA-33pg-m6jh-5237, https://github.com/moby/moby/pull/45118	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incoming and outgoing IPSec. These rules rely on the `u32` iptables extension provided by the `xt_u32` kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. An iptables rule designates outgoing VXLAN datagrams with a VNI that corresponds to an encrypted overlay network for IPsec encapsulation. Encrypted overlay networks on affected platforms silently transmit unencrypted data. As a result, `overlay` networks may appear to be functional, passing traffic as expected, but without any of the expected confidentiality or data integrity guarantees. It is possible for an attacker sitting in a trusted position on		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the network to read all of the application traffic that is moving across the overlay network, resulting in unexpected secrets or user data disclosure. Thus, because many database protocols, internal APIs, etc. are not protected by a second layer of encryption, a user may use Swarm encrypted overlay networks to provide confidentiality, which due to this vulnerability this is no longer guaranteed. Patches are available in Moby releases 23.0.3, and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. Close the VXLAN port (by default, UDP port 4789) to outgoing traffic at the Internet boundary in order to prevent unintentionally leaking unencrypted traffic over the Internet, and/or ensure that the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`xt_u32` kernel module is available on all nodes of the Swarm cluster. **CVE ID : CVE-2023-28841**		
Improper Handling of Exceptional Conditions	04-Apr-2023	6.8	Moby) is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon component (`dockerd`), which is developed as moby/moby is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in `dockerd` and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The `overlay` network driver is a core feature of Swarm Mode,	https://github.com/moby/moby/security/advisories/GHSA-6wrf-mxfj-pf5p, https://github.com/moby/libnetwork/security/advisories/GHSA-gvm4-2qqg-m333, https://github.com/moby/moby/security/advisories/GHSA-vwm3-crmr-xfxw	A-MOB-MOBY-200423/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with the VXLAN metadata, including a VXLAN Network ID (VNI) that identifies the originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both incoming and outgoing IPSec. These rules rely on the `u32` iptables extension provided by the `xt_u32` kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. The `overlay` driver dynamically and lazily defines the kernel configuration for the VXLAN network on each node as containers		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are attached and detached. Routes and encryption parameters are only defined for destination nodes that participate in the network. The iptables rules that prevent encrypted overlay networks from accepting unencrypted packets are not created until a peer is available with which to communicate. Encrypted overlay networks silently accept cleartext VXLAN datagrams that are tagged with the VNI of an encrypted overlay network. As a result, it is possible to inject arbitrary Ethernet frames into the encrypted overlay network by encapsulating them in VXLAN datagrams. The implications of this can be quite dire, and GHSA-vwm3-crmr-xfxw should be referenced for a deeper exploration. Patches are available in Moby releases 23.0.3, and 20.10.24. As Mirantis Container Runtime's 20.10 releases are		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. In multi-node clusters, deploy a global 'pause' container for each encrypted overlay network, on every node. For a single-node cluster, do not use overlay networks of any sort. Bridge networks provide the same connectivity on a single node and have no multi-node features. The Swarm ingress feature is implemented using an overlay network, but can be disabled by publishing ports in `host` mode instead of `ingress` mode (allowing the use of an external load balancer), and removing the `ingress` network. If encrypted overlay networks are in exclusive use, block UDP port 4789 from traffic that has not been validated by IPSec. **CVE ID : CVE-2023-28842**		
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.3					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	04-Apr-2023	8.7	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon component (`dockerd`), which is developed as moby/moby, is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in dockerd and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The overlay network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This	https://github.com/moby/libnetwork/security/advisories/GHSA-gvm4-2qqg-m333, https://github.com/moby/moby/security/advisories/GHSA-232p-vwff-86mp, https://github.com/moby/moby/security/advisories/GHSA-vwm3-crmr-xfxw, https://github.com/moby/moby/pull/45118	A-MOB-MOBY-200423/385

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with a VXLAN Network ID (VNI) that identifies the originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both incoming and outgoing IPSec. These rules rely on the u32 iptables extension provided by the xt_u32 kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. Two iptables rules serve to filter incoming VXLAN datagrams with a VNI that corresponds to an encrypted network and discards unencrypted datagrams. The rules are appended to the end of the INPUT filter chain, following any rules that have been previously set by the system administrator.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	Administrator-set rules take precedence over the rules Moby sets to discard unencrypted VXLAN datagrams, which can potentially admit unencrypted datagrams that should have been discarded. The injection of arbitrary Ethernet frames can enable a Denial of Service attack. A sophisticated attacker may be able to establish a UDP or TCP connection by way of the container’s outbound gateway that would otherwise be blocked by a stateful firewall, or carry out other escalations beyond simple injection by smuggling packets into the overlay network. Patches are available in Moby releases 23.0.3 and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. Close the VXLAN port (by default, UDP port		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4789) to incoming traffic at the Internet boundary to prevent all VXLAN packet injection, and/or ensure that the `xt_u32` kernel module is available on all nodes of the Swarm cluster. **CVE ID : CVE-2023-28840**		
Missing Encryption of Sensitive Data	04-Apr-2023	6.8	Moby is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon component (`dockerd`), which is developed as moby/moby is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in `dockerd` and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of	https://github.com/moby/libnetwork/security/advisories/GHSA-gvm4-2qqg-m333, https://github.com/moby/moby/security/advisories/GHSA-vwm3-crmr-xfxw, https://github.com/moby/moby/security/advisories/GHSA-33pg-m6jh-5237, https://github.com/moby/moby/pull/45118	A-MOB-MOBY-200423/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SwarmKit and supporting network code. The `overlay` network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with the VXLAN metadata, including a VXLAN Network ID (VNI) that identifies the originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both incoming and outgoing IPSec. These rules rely on the `u32` iptables extension provided by the `xt_u32` kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. An iptables rule		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			designates outgoing VXLAN datagrams with a VNI that corresponds to an encrypted overlay network for IPsec encapsulation. Encrypted overlay networks on affected platforms silently transmit unencrypted data. As a result, `overlay` networks may appear to be functional, passing traffic as expected, but without any of the expected confidentiality or data integrity guarantees. It is possible for an attacker sitting in a trusted position on the network to read all of the application traffic that is moving across the overlay network, resulting in unexpected secrets or user data disclosure. Thus, because many database protocols, internal APIs, etc. are not protected by a second layer of encryption, a user may use Swarm encrypted overlay networks to provide confidentiality, which due to this		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability this is no longer guaranteed. Patches are available in Moby releases 23.0.3, and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. Close the VXLAN port (by default, UDP port 4789) to outgoing traffic at the Internet boundary in order to prevent unintentionally leaking unencrypted traffic over the Internet, and/or ensure that the `xt_u32` kernel module is available on all nodes of the Swarm cluster. **CVE ID : CVE-2023-28841**		
Improper Handling of Exceptional Conditions	04-Apr-2023	6.8	Moby) is an open source container framework developed by Docker Inc. that is distributed as Docker, Mirantis Container Runtime, and various other downstream projects/products. The Moby daemon	https://github.com/moby/moby/security/advisories/GHSA-6wrf-mxfj-pf5p, https://github.com/moby/libnetwork/security/advisories/GHSA-gvm4-2qqg-	A-MOB-MOBY-200423/387

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component (`dockerd`), which is developed as moby/moby is commonly referred to as *Docker*. Swarm Mode, which is compiled in and delivered by default in `dockerd` and is thus present in most major Moby downstreams, is a simple, built-in container orchestrator that is implemented through a combination of SwarmKit and supporting network code. The `overlay` network driver is a core feature of Swarm Mode, providing isolated virtual LANs that allow communication between containers and services across the cluster. This driver is an implementation/user of VXLAN, which encapsulates link-layer (Ethernet) frames in UDP datagrams that tag the frame with the VXLAN metadata, including a VXLAN Network ID (VNI) that identifies the	m333, https://github.com/moby/moby/security/advisories/GHSA-vwm3-crmr-xfxw	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			originating overlay network. In addition, the overlay network driver supports an optional, off-by-default encrypted mode, which is especially useful when VXLAN packets traverses an untrusted network between nodes. Encrypted overlay networks function by encapsulating the VXLAN datagrams through the use of the IPsec Encapsulating Security Payload protocol in Transport mode. By deploying IPSec encapsulation, encrypted overlay networks gain the additional properties of source authentication through cryptographic proof, data integrity through check-summing, and confidentiality through encryption. When setting an endpoint up on an encrypted overlay network, Moby installs three iptables (Linux kernel firewall) rules that enforce both		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incoming and outgoing IPSec. These rules rely on the `u32` iptables extension provided by the `xt_u32` kernel module to directly filter on a VXLAN packet's VNI field, so that IPSec guarantees can be enforced on encrypted overlay networks without interfering with other overlay networks or other users of VXLAN. The `overlay` driver dynamically and lazily defines the kernel configuration for the VXLAN network on each node as containers are attached and detached. Routes and encryption parameters are only defined for destination nodes that participate in the network. The iptables rules that prevent encrypted overlay networks from accepting unencrypted packets are not created until a peer is available with which to communicate. Encrypted overlay networks silently		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accept cleartext VXLAN datagrams that are tagged with the VNI of an encrypted overlay network. As a result, it is possible to inject arbitrary Ethernet frames into the encrypted overlay network by encapsulating them in VXLAN datagrams. The implications of this can be quite dire, and GHSA-vwm3-crmr-xfxw should be referenced for a deeper exploration. Patches are available in Moby releases 23.0.3, and 20.10.24. As Mirantis Container Runtime's 20.10 releases are numbered differently, users of that platform should update to 20.10.16. Some workarounds are available. In multi-node clusters, deploy a global 'pause' container for each encrypted overlay network, on every node. For a single-node cluster, do not use overlay networks of any sort. Bridge networks provide the same connectivity on a single node and have		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			no multi-node features. The Swarm ingress feature is implemented using an overlay network, but can be disabled by publishing ports in `host` mode instead of `ingress` mode (allowing the use of an external load balancer), and removing the `ingress` network. If encrypted overlay networks are in exclusive use, block UDP port 4789 from traffic that has not been validated by IPSec. **CVE ID : CVE-2023-28842**		
Vendor: modal_dialog_project					
Product: modal_dialog					
Affected Version(s): * Up to (excluding) 3.5.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Yannick Lefebvre Modal Dialog plugin <= 3.5.9 versions. **CVE ID : CVE-2023-24001**	N/A	A-MOD-MODA-200423/388
Vendor: monitorr_project					
Product: monitorr					
Affected Version(s): 1.7.6m					
Unrestricted Upload of File with	04-Apr-2023	7.8	File Upload vulnerability found in Monitorr v.1.7.6	N/A	A-MON-MONI-200423/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			allows a remote attacker t oexecute arbitrary code via a crafted file upload to the assets/php/upload.php endpoint. **CVE ID : CVE-2023-26775**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	6.1	Cross Site Scripting vulnerability found in Monitorr v.1.7.6 allows a remote attacker to execute arbitrary code via the title parameter of the post_receiver-services.php file. **CVE ID : CVE-2023-26776**	N/A	A-MON-MONI-200423/390
Vendor: multi-column_tag_map_project					
Product: multi-column_tag_map					
Affected Version(s): * Up to (excluding) 17.0.25					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Alan Jackson Multi-column Tag Map plugin <= 17.0.24 versions. **CVE ID : CVE-2023-23815**	N/A	A-MUL-MULT-200423/391
Vendor: my-blog_project					
Product: my-blog					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	07-Apr-2023	4.3	A vulnerability, which was classified as problematic, was found in zhenfeng13	N/A	A-MY--MY-B-200423/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			My-Blog. Affected is an unknown function of the file /admin/configurations/userInfo. The manipulation of the argument yourAvatar/yourName/yourEmail leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-225264. **CVE ID : CVE-2023-1937**		
Vendor: mybatis					
Product: mybatis					
Affected Version(s): * Up to (excluding) 3.5.3.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	9.8	A SQL injection vulnerability in Mybatis plus below 3.5.3.1 allows remote attackers to execute arbitrary SQL commands via the tenant ID valuer. **CVE ID : CVE-2023-25330**	N/A	A-MYB-MYBA-200423/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Nextcloud					
Product: desktop					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.6.5					
Reusing a Nonce, Key Pair in Encryption	04-Apr-2023	6.5	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with version 3.0.0 and prior to version 3.6.5, a malicious server administrator can recover and modify the contents of end-to-end encrypted files. Users should upgrade the Nextcloud Desktop client to 3.6.5 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-28997**	https://github.com/nextcloud/desktop/pull/5324, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-4p33-rw27-j5fc	A-NEX-DESK-200423/394
Missing Cryptographic Step	04-Apr-2023	6.1	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with version 3.0.0 and prior to version 3.6.5, a malicious server administrator can gain full access to an end-to-end encrypted folder. They can decrypt files, recover the folder structure, and add new files.? Users should upgrade the	https://github.com/nextcloud/desktop/pull/5323, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-jh3g-wpwv-cqgr	A-NEX-DESK-200423/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nextcloud Desktop client to 3.6.5 to receive a patch. No known workarounds are available. **CVE ID : CVE-2023-28998**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.7.0					
Improper Certificate Validation	04-Apr-2023	6.5	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server. Starting with version 3.0.0 and prior to version 3.7.0, by trusting that the server will return a certificate that belongs to the keypair of the user, a malicious server could get the desktop client to encrypt files with a key known to the attacker. This issue is fixed in Nextcloud Desktop 3.7.0. No known workarounds are available. **CVE ID : CVE-2023-29000**	https://github.com/nextcloud/desktop/pull/4949, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-h82x-98q3-7534	A-NEX-DESK-200423/396
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.8.0					
Missing Encryption of Sensitive Data	04-Apr-2023	6.4	Nextcloud is an open-source productivity platform. In Nextcloud Desktop client 3.0.0 until 3.8.0, Nextcloud Android app 3.13.0 until 3.25.0, and	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8875-wxww-3rr8, https://github	A-NEX-DESK-200423/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Nextcloud iOS app 3.0.5 until 4.8.0, a malicious server administrator can gain full access to an end-to-end encrypted folder. They can decrypt files, recover the folder structure and add new files.? This issue is fixed in Nextcloud Desktop 3.8.0, Nextcloud Android 3.25.0, and Nextcloud iOS 4.8.0. No known workarounds are available. **CVE ID : CVE-2023-28999**	.com/nextcloud/desktop/pull/5560	
Product: nextcloud					
Affected Version(s): From (including) 3.0.5 Up to (excluding) 4.8.0					
Missing Encryption of Sensitive Data	04-Apr-2023	6.4	Nextcloud is an open-source productivity platform. In Nextcloud Desktop client 3.0.0 until 3.8.0, Nextcloud Android app 3.13.0 until 3.25.0, and Nextcloud iOS app 3.0.5 until 4.8.0, a malicious server administrator can gain full access to an end-to-end encrypted folder. They can decrypt files, recover the folder structure and add new files.? This	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8875-wxww-3rr8, https://github.com/nextcloud/desktop/pull/5560	A-NEX-NEXT-200423/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in Nextcloud Desktop 3.8.0, Nextcloud Android 3.25.0, and Nextcloud iOS 4.8.0. No known workarounds are available. **CVE ID : CVE-2023-28999**		
Affected Version(s): From (including) 3.13.0 Up to (excluding) 3.25.0					
Missing Encryption of Sensitive Data	04-Apr-2023	6.4	Nextcloud is an open-source productivity platform. In Nextcloud Desktop client 3.0.0 until 3.8.0, Nextcloud Android app 3.13.0 until 3.25.0, and Nextcloud iOS app 3.0.5 until 4.8.0, a malicious server administrator can gain full access to an end-to-end encrypted folder. They can decrypt files, recover the folder structure and add new files.? This issue is fixed in Nextcloud Desktop 3.8.0, Nextcloud Android 3.25.0, and Nextcloud iOS 4.8.0. No known workarounds are available. **CVE ID : CVE-2023-28999**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-8875-wxww-3rr8, https://github.com/nextcloud/desktop/pull/5560	A-NEX-NEXT-200423/399
Product: nextcloud_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.14					
Improper Removal of Sensitive Information Before Storage or Transfer	03-Apr-2023	4.3	Nextcloud Server is an open source personal cloud server. Nextcloud Server 24.0.0 until 24.0.6 and 25.0.0 until 25.0.4, as well as Nextcloud Enterprise Server 23.0.0 until 23.0.11, 24.0.0 until 24.0.6, and 25.0.0 until 25.0.4, have an information disclosure vulnerability. A user was able to get the full data directory path of the Nextcloud server from an API endpoint. By itself this information is not problematic as it can also be guessed for most common setups, but it could speed up other unknown attacks in the future if the information is known. Nextcloud Server 24.0.6 and 25.0.4 and Nextcloud Enterprise Server 23.0.11, 24.0.6, and 25.0.4 contain patches for this issue. There are no known workarounds. **CVE ID : CVE-2023-28834**	https://hackerone.com/reports/1690510 , https://github.com/nextcloud/server/pull/36094, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-5w64-6c42-rgcv	A-NEX-NEXT-200423/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.10					
Improper Removal of Sensitive Information Before Storage or Transfer	03-Apr-2023	4.3	Nextcloud Server is an open source personal cloud server. Nextcloud Server 24.0.0 until 24.0.6 and 25.0.0 until 25.0.4, as well as Nextcloud Enterprise Server 23.0.0 until 23.0.11, 24.0.0 until 24.0.6, and 25.0.0 until 25.0.4, have an information disclosure vulnerability. A user was able to get the full data directory path of the Nextcloud server from an API endpoint. By itself this information is not problematic as it can also be guessed for most common setups, but it could speed up other unknown attacks in the future if the information is known. Nextcloud Server 24.0.6 and 25.0.4 and Nextcloud Enterprise Server 23.0.11, 24.0.6, and 25.0.4 contain patches for this issue. There are no known workarounds. **CVE ID : CVE-2023-28834**	https://hackerone.com/reports/1690510 , https://github.com/nextcloud/server/pull/36094, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-5w64-6c42-rgcv	A-NEX-NEXT-200423/401

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.4					
Improper Removal of Sensitive Information Before Storage or Transfer	03-Apr-2023	4.3	Nextcloud Server is an open source personal cloud server. Nextcloud Server 24.0.0 until 24.0.6 and 25.0.0 until 25.0.4, as well as Nextcloud Enterprise Server 23.0.0 until 23.0.11, 24.0.0 until 24.0.6, and 25.0.0 until 25.0.4, have an information disclosure vulnerability. A user was able to get the full data directory path of the Nextcloud server from an API endpoint. By itself this information is not problematic as it can also be guessed for most common setups, but it could speed up other unknown attacks in the future if the information is known. Nextcloud Server 24.0.6 and 25.0.4 and Nextcloud Enterprise Server 23.0.11, 24.0.6, and 25.0.4 contain patches for this issue. There are no known workarounds. **CVE ID : CVE-2023-28834**	https://hackerone.com/reports/1690510 , https://github.com/nextcloud/server/pull/36094, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-5w64-6c42-rgcv	A-NEX-NEXT-200423/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: user_oidc					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.3.0					
Cross-Site Request Forgery (CSRF)	04-Apr-2023	5.4	user_oidc is the OIDC connect user backend for Nextcloud, an open source collaboration platform. A vulnerability in versions 1.0.0 until 1.3.0 effectively allowed an attacker to bypass the state protection as they could just copy the expected state token from the first request to their second request. Users should upgrade user_oidc to 1.3.0 to receive a patch for the issue. No known workarounds are available. **CVE ID : CVE-2023-28848**	https://github.com/nextcloud/user_oidc/pull/580, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-52hv-xw32-wf7f	A-NEX-USER-200423/403
Vendor: nlb-creations					
Product: scheduled_announcements_widget					
Affected Version(s): * Up to (excluding) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	The Scheduled Announcements Widget WordPress plugin before 1.0 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow	N/A	A-NLB-SCHE-200423/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users with the contributor role and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-0363**		
Vendor: nophp_project					
Product: nophp					
Affected Version(s): * Up to (excluding) 0.0.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Apr-2023	8.8	nophp is a PHP web framework. Prior to version 0.0.1, nophp is vulnerable to shell command injection on httpd user. A patch was made available at commit e5409aa2d441789cbb35f6b119bef97ecc3986aa on 2023-03-30. Users should update index.php to 2023-03-30 or later or, as a workaround, add a function such as `env_patchsample230330.php` to env.php. **CVE ID : CVE-2023-28854**	https://github.com/paijp/nophp/security/advisories/GHSA-9858-q3c2-9wwm, https://github.com/paijp/nophp/commit/e5409aa2d441789cbb35f6b119bef97ecc3986aa	A-NOP-NOPH-200423/405
Vendor: novisurvey					
Product: novi_survey					
Affected Version(s): * Up to (excluding) 8.9.43676					
Improper Control of Generation of Code	11-Apr-2023	9.8	Novi Survey before 8.9.43676 allows remote attackers to execute arbitrary code on the server in the context of the	https://novisurvey.net/blog/novi-survey-security-	A-NOV-NOVI-200423/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			service account. This does not provide access to stored survey or response data. **CVE ID : CVE-2023-29492**	advisory-apr-2023.aspx	
Vendor: Nvidia					
Product: data_center_gpu_manager					
Affected Version(s): * Up to (excluding) 3.1.7					
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA DCGM for Linux contains a vulnerability in HostEngine (server component) where a user may cause a heap-based buffer overflow through the bound socket. A successful exploit of this vulnerability may lead to denial of service and data tampering. **CVE ID : CVE-2023-0208**	https://nvidia.custhelp.com/app/answers/detail/a_id/5453	A-NVI-DATA-200423/407
Product: virtual_gpu					
Affected Version(s): * Up to (excluding) 11.12					
Out-of-bounds Write	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service, information disclosure, and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0182		
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering. **CVE ID : CVE-2023-0189**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/409
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer handler, where improper privilege management can lead to escalation of privileges and information disclosure. **CVE ID : CVE-2023-0192**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/410
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a memory buffer can lead to denial of	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, information disclosure, and data tampering. **CVE ID : CVE-2023-0198**		
N/A	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in a kernel mode layer handler, which may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0180**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/412
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/413
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of service and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0183		
Incorrect Conversion between Numeric Types	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where sign conversion issuescasting an unsigned primitive to signed may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0185**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/415
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service and data tampering. **CVE ID : CVE-2023-0186**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/416
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Apr-2023	6.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious user in a guest VM can cause a NULL-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2023-0197**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/418
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds read can lead to denial of service. **CVE ID : CVE-2023-0187**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/419
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service. **CVE ID : CVE-2023-0188**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Apr-2023	4.6	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer driver, where an invalid display configuration may lead to denial of service. **CVE ID : CVE-2023-0194**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/421
Improper Validation of Specified Quantity in Input	01-Apr-2023	2.4	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer driver nvlddmkm.sys, where an can cause CWE-1284, which may lead to hypothetical Information leak of unimportant data such as local variable data of the driver **CVE ID : CVE-2023-0195**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/422
Affected Version(s): From (including) 13.0 Up to (excluding) 13.7					
Out-of-bounds Write	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service, information disclosure, and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0182		
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering. **CVE ID : CVE-2023-0189**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/424
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer handler, where improper privilege management can lead to escalation of privileges and information disclosure. **CVE ID : CVE-2023-0192**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/425
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a memory buffer can lead to denial of	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, information disclosure, and data tampering. **CVE ID : CVE-2023-0198**		
N/A	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in a kernel mode layer handler, which may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0180**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/427
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/428
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of service and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0183		
Incorrect Conversion between Numeric Types	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where sign conversion issuescasting an unsigned primitive to signed may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0185**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/430
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service and data tampering. **CVE ID : CVE-2023-0186**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/431
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Apr-2023	6.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious user in a guest VM can cause a NULL-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2023-0197**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/433
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds read can lead to denial of service. **CVE ID : CVE-2023-0187**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/434
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service. **CVE ID : CVE-2023-0188**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Apr-2023	4.6	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer driver, where an invalid display configuration may lead to denial of service. **CVE ID : CVE-2023-0194**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/436
Improper Validation of Specified Quantity in Input	01-Apr-2023	2.4	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer driver nvlddmkm.sys, where an can cause CWE-1284, which may lead to hypothetical Information leak of unimportant data such as local variable data of the driver **CVE ID : CVE-2023-0195**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/437
Affected Version(s): From (including) 15.0 Up to (excluding) 15.2					
Out-of-bounds Write	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service, information disclosure, and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0182		
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering. **CVE ID : CVE-2023-0189**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/439
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer handler, where improper privilege management can lead to escalation of privileges and information disclosure. **CVE ID : CVE-2023-0192**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/440
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a memory buffer can lead to denial of	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, information disclosure, and data tampering. **CVE ID : CVE-2023-0198**		
N/A	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in a kernel mode layer handler, which may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0180**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/442
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/443
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of service and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0183		
Incorrect Conversion between Numeric Types	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where sign conversion issuescasting an unsigned primitive to signed may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0185**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/445
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service and data tampering. **CVE ID : CVE-2023-0186**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/446
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-Apr-2023	6.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious user in a guest VM can cause a NULL-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2023-0197**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/448
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds read can lead to denial of service. **CVE ID : CVE-2023-0187**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/449
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service. **CVE ID : CVE-2023-0188**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	01-Apr-2023	4.6	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer driver, where an invalid display configuration may lead to denial of service. **CVE ID : CVE-2023-0194**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/451
Improper Validation of Specified Quantity in Input	01-Apr-2023	2.4	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer driver nvlddmkm.sys, where an can cause CWE-1284, which may lead to hypothetical Information leak of unimportant data such as local variable data of the driver **CVE ID : CVE-2023-0195**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	A-NVI-VIRT-200423/452
Vendor: oceanwp					
Product: ocean_extra					
Affected Version(s): * Up to (excluding) 2.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in OceanWP Ocean Extra plugin <= 2.1.1 versions. Needs the OceanWP theme	N/A	A-OCE-OCEA-200423/453

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installed and activated. **CVE ID : CVE-2023-23891**		
Vendor: online_computer_and_laptop_store_project					
Product: online_computer_and_laptop_store					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	04-Apr-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file php-ocls\admin\system_info\index.php. The manipulation of the argument img leads to unrestricted upload. It is possible to initiate the attack remotely. The identifier VDB-224841 was assigned to this vulnerability. **CVE ID : CVE-2023-1826**	N/A	A-ONL-ONLI-200423/454
Unrestricted Upload of File with Dangerous Type	07-Apr-2023	9.8	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/?page=user	N/A	A-ONL-ONLI-200423/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the component Avatar Handler. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225319. **CVE ID : CVE-2023-1942**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	9.8	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this issue is the function delete_brand of the file /admin/maintenance/brand.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-225338 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1951**	N/A	A-ONL-ONLI-200423/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	9.8	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been classified as critical. This affects an unknown part of the file /?p=products of the component Product Search. The manipulation of the argument search leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225339. **CVE ID : CVE-2023-1952**	N/A	A-ONL-ONLI-200423/457
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected is an unknown function of the file login.php of the component User Registration. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to	N/A	A-ONL-ONLI-200423/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. VDB-225342 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1955**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Computer and Laptop Store 1.0. This affects an unknown part of the file /classes/Master.php?f=delete_sub_category. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225345 was assigned to this vulnerability. **CVE ID : CVE-2023-1958**	N/A	A-ONL-ONLI-200423/459
Improper Neutralization of Special Elements used in an SQL Command	08-Apr-2023	8.8	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been declared as critical. This vulnerability affects unknown code of the file	N/A	A-ONL-ONLI-200423/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			/admin/sales/index.php. The manipulation of the argument date_start/date_end leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225340. **CVE ID : CVE-2023-1953**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	8.8	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been rated as critical. This issue affects the function save_inventory of the file /admin/product/manage.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225341 was assigned to this vulnerability. **CVE ID : CVE-2023-1954**	N/A	A-ONL-ONLI-200423/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Apr-2023	8.8	A vulnerability classified as critical was found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=delete_img of the component Image Handler. The manipulation of the argument path leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225343. **CVE ID : CVE-2023-1956**	N/A	A-ONL-ONLI-200423/462
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=save_sub_category of the component	N/A	A-ONL-ONLI-200423/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Subcategory Handler. The manipulation of the argument sub_category leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225344. **CVE ID : CVE-2023-1957**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	8.8	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This vulnerability affects unknown code of the file /classes/Master.php?f=save_category. The manipulation of the argument category leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-225346 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1959**	N/A	A-ONL-ONLI-200423/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Apr-2023	8.8	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Master.php ?f=delete_category. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225347. **CVE ID : CVE-2023-1960**	N/A	A-ONL-ONLI-200423/465
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Apr-2023	7.2	A vulnerability, which was classified as critical, has been found in SourceCodester Online Computer and Laptop Store 1.0. This issue affects the function save_brand of the file /classes/Master.php ?f=save_brand. The manipulation of the argument name leads to sql injection. The attack may be initiated remotely. The exploit has been	N/A	A-ONL-ONLI-200423/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier VDB-225533 was assigned to this vulnerability. **CVE ID : CVE-2023-1985**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Apr-2023	7.2	A vulnerability, which was classified as critical, was found in SourceCodester Online Computer and Laptop Store 1.0. Affected is the function delete_order of the file /classes/master.php?f=delete_order. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225534 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1986**	N/A	A-ONL-ONLI-200423/467
Improper Neutralization of Special Elements used in an SQL Command	11-Apr-2023	7.2	A vulnerability has been found in SourceCodester Online Computer and Laptop Store 1.0 and classified as critical. Affected by this vulnerability is the function	N/A	A-ONL-ONLI-200423/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			update_order_status of the file /classes/Master.php?f=update_order_status. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-225535. **CVE ID : CVE-2023-1987**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/?page=product/manage_product&id=2. The manipulation of the argument Product Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier	N/A	A-ONL-ONLI-200423/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability is VDB-224996. **CVE ID : CVE-2023-1857**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Apr-2023	6.1	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/?page=system_info. The manipulation of the argument System Name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225348. **CVE ID : CVE-2023-1961**	N/A	A-ONL-ONLI-200423/470
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	4.8	A vulnerability was found in SourceCodester Online Computer and Laptop Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/?page=maintenance/brand. The	N/A	A-ONL-ONLI-200423/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument Brand Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225536. **CVE ID : CVE-2023-1988**		
Vendor: online_eyewear_shop_project					
Product: online_eyewear_shop					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Apr-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. This vulnerability affects unknown code of the file /admin/inventory/manage_stock.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-225406 is the identifier assigned to this vulnerability.	N/A	A-ONL-ONLI-200423/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1969		
Vendor: online_graduate_tracer_system_project					
Product: online_graduate_tracer_system					
Affected Version(s): 1.0					
Insufficient Session Expiration	05-Apr-2023	9.8	A vulnerability, which was classified as problematic, was found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file admin/. The manipulation leads to session expiration. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-224994 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1854**	N/A	A-ONL-ONLI-200423/473
Vendor: online_payroll_system_project					
Product: online_payroll_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Online Payroll System 1.0. This affects an unknown part of the file /admin/employee_row.php. The	N/A	A-ONL-ONLI-200423/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224985 was assigned to this vulnerability. **CVE ID : CVE-2023-1845**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	9.8	A vulnerability has been found in SourceCodester Online Payroll System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/deduction_row.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-224986 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1846**	N/A	A-ONL-ONLI-200423/475
Improper Neutralization of Special	05-Apr-2023	9.8	A vulnerability was found in SourceCodester Online Payroll	N/A	A-ONL-ONLI-200423/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			System 1.0 and classified as critical. This issue affects some unknown processing of the file attendance.php. The manipulation of the argument employee leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224987. **CVE ID : CVE-2023-1847**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	9.8	A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/attendance_row.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224988.	N/A	A-ONL-ONLI-200423/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1848		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	9.8	A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/cashadvance_row.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224989 was assigned to this vulnerability. **CVE ID : CVE-2023-1849**	N/A	A-ONL-ONLI-200423/478
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Apr-2023	9.8	A vulnerability was found in SourceCodester Online Payroll System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/login.php. The manipulation of the argument username leads to	N/A	A-ONL-ONLI-200423/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-224990 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1850**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Online Payroll System 1.0. This affects an unknown part of the file /admin/employee_add.php. The manipulation of the argument of leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224991. **CVE ID : CVE-2023-1851**	N/A	A-ONL-ONLI-200423/480
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	A vulnerability classified as problematic was found in SourceCodester Online Payroll	N/A	A-ONL-ONLI-200423/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			System 1.0. This vulnerability affects unknown code of the file /admin/deduction_edit.php. The manipulation of the argument description leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-224992. **CVE ID : CVE-2023-1852**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Online Payroll System 1.0. This issue affects some unknown processing of the file /admin/employee_edit.php. The manipulation of the argument of leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224993 was assigned to this vulnerability. **CVE ID : CVE-2023-1853**	N/A	A-ONL-ONLI-200423/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: opencats					
Product: opencats					
Affected Version(s): 0.9.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	A stored cross-site scripting (XSS) vulnerability in OpenCATS v0.9.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the city parameter at opencats/index.php?m=candidates. **CVE ID : CVE-2023-26846**	http://opencats.com	A-OPE-OPEN-200423/483
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	A stored cross-site scripting (XSS) vulnerability in OpenCATS v0.9.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the state parameter at opencats/index.php?m=candidates. **CVE ID : CVE-2023-26847**	https://opencats.org	A-OPE-OPEN-200423/484
Cross-Site Request Forgery (CSRF)	11-Apr-2023	4.3	A Cross-Site Request Forgery (CSRF) in OpenCATS 0.9.7 allows attackers to force users into submitting web requests via unspecified vectors. **CVE ID : CVE-2023-26845**	http://opencats.com	A-OPE-OPEN-200423/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: opendesign					
Product: drawings_sdk					
Affected Version(s): * Up to (excluding) 2024.1					
Use After Free	10-Apr-2023	7.8	An issue was discovered in Open Design Alliance Drawings SDK before 2024.1. A crafted DWG file can force the SDK to reuse an object that has been freed. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code. **CVE ID : CVE-2023-26495**	https://www.opendesign.com/security-advisories	A-OPE-DRAW-200423/486
Vendor: opensmtpd					
Product: opensmtpd					
Affected Version(s): * Up to (excluding) 7.0.0					
N/A	04-Apr-2023	7.8	ascii_load_sockaddr in smtpd in OpenBSD before 7.1 errata 024 and 7.2 before errata 020, and OpenSMTPD Portable before 7.0.0-portable commit f748277, can abort upon a connection from a local, scoped IPv6 address. **CVE ID : CVE-2023-29323**	https://ftp.openbsd.org/pub/OpenBSD/patches/7.2/common/020_smtpd.patch.sig, https://ftp.openbsd.org/pub/OpenBSD/patches/7.1/common/024_smtpd.patch.sig, https://github.com/OpenSMTPD/OpenSMTPD/commit/41d0eae481f5	A-OPE-OPEN-200423/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				38956b1f1fbadfb535043454061f	
Vendor: openwrt					
Product: luci					
Affected Version(s): 22.03.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	LuCI openwrt-22.03 branch git-22.361.69894-438c598 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the component /openvpn/pageswitch.htm. **CVE ID : CVE-2023-24181**	https://github.com/openwrt/luci/commit/749268a2cad4a08722e30f66a578e254885f450f, https://github.com/openwrt/luci/commit/25983b9fa572a640a7ecd077378df2790266cd61	A-OPE-LUCI-200423/488
Product: openwrt					
Affected Version(s): 22.03.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	LuCI openwrt-22.03 branch git-22.361.69894-438c598 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the component /system/sshkeys.js. **CVE ID : CVE-2023-24182**	https://github.com/openwrt/luci/commit/0186d7eae0e123a409e9919a83fdfecc7945c984, https://github.com/openwrt/luci/commit/588381e2111079265cc3b20af33507052f1b58cb, https://github.com/openwrt/luci/commit/aa7938d4cb3a3f889dead89	A-OPE-OPEN-200423/489

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4ea19334ad0 7ade51	
Vendor: orangescrum					
Product: orangescrum					
Affected Version(s): 2.0.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	6.1	OrangeScrum version 2.0.11 allows an external attacker to obtain arbitrary user accounts from the application. This is possible because the application returns malicious user input in the response with the content-type set to text/html. **CVE ID : CVE-2023-0738**	N/A	A-ORA-ORAN-200423/490
Vendor: otcms					
Product: otcms					
Affected Version(s): 6.01					
Unrestricted Upload of File with Dangerous Type	02-Apr-2023	9.8	A vulnerability classified as critical was found in OTCMS 6.0.1. Affected by this vulnerability is an unknown functionality of the file sysCheckFile.php?mudi=sql. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The	N/A	A-OTC-OTCM-200423/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier VDB-224749 was assigned to this vulnerability. **CVE ID : CVE-2023-1797**		
Vendor: pega					
Product: synchronization_engine					
Affected Version(s): From (including) 3.1.1 Up to (excluding) 3.1.30					
N/A	10-Apr-2023	7.8	A user with non-Admin access can change a configuration file on the client to modify the Server URL. **CVE ID : CVE-2023-26466**	https://support.pega.com/support-doc/pega-security-advisory-b23-robotics-and-workforce-intelligence-local-privilege	A-PEG-SYNC-200423/492
Vendor: pgyer					
Product: codefever					
Affected Version(s): * Up to (excluding) 2023-02-07					
N/A	07-Apr-2023	8.8	codefever before 2023.2.7-commit-b1c2e7f was discovered to contain a remote code execution (RCE) vulnerability via the component /controllers/api/user.php. **CVE ID : CVE-2023-26817**	N/A	A-PGY-CODE-200423/493
Vendor: Phpmyfaq					
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.1.12					
Authentication	05-Apr-2023	9.8	Authentication Bypass by Capture-	https://huntr.dev/bounties/	A-PHP-PHPM-200423/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bypass by Capture-replay			replay in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1886**	b7d244b7-5ac3-4964-81ee-8dbb5bb5e33a, https://github.com/thorsten/phpmyfaq/commit/27eaaae16850694634ac52416a0bd38b35d7330a	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1880**	https://huntr.dev/bounties/ece5f051-674e-4919-b998-594714910f9e, https://github.com/thorsten/phpmyfaq/commit/bbc5d4aa4a4375c14e34dd9fcad2042066fe476d	A-PHP-PHPM-200423/495
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Cross-site Scripting (XSS) - Generic in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1884**	https://github.com/thorsten/phpmyfaq/commit/7f0f921de74c88038826c46bbd2a123518d9d611, https://huntr.dev/bounties/dda73cb6-9344-4822-97a1-2e31efb6a73e	A-PHP-PHPM-200423/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1756**	https://huntr.dev/bounties/e495b443-b328-42f5-aed5-d68b929b4cb9, https://github.com/thorsten/phpmyfaq/commit/ca75f4688a8b0f14d5d0697b9f4b6ea66088f726	A-PHP-PHPM-200423/497
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1757**	https://github.com/thorsten/phpmyfaq/commit/5061e5841be6c218ebb0de0cbf7b7f195dc46d19, https://huntr.dev/bounties/584a200a-6ff8-4d53-a3c0-e7893edff60c	A-PHP-PHPM-200423/498
Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)	05-Apr-2023	5.4	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1758**	https://github.com/thorsten/phpmyfaq/commit/f3380f46c464d1bc6f3ded29213c79be0de8fc57, https://huntr.dev/bounties/0854328e-eb00-41a3-9573-8da8f00e369c	A-PHP-PHPM-200423/499
Improper Neutralizat	05-Apr-2023	5.4	Cross-site Scripting (XSS) - Stored in	https://huntr.dev/bounties/	A-PHP-PHPM-200423/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1878**	93f981a3-231d-460d-a239-bb960e8c2fdc, https://github.com/thorsten/phpmyfaq/commit/e018823f8e3bca103c11e5a98b0dd469e41ed417	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1879**	https://huntr.dev/bounties/1dc7f818-c8ea-4f80-b000-31b48a426334, https://github.com/thorsten/phpmyfaq/commit/0dc8e527c375007cd4b8dbf61f7167393a6f6e91	A-PHP-PHPM-200423/501
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Cross-site Scripting (XSS) - DOM in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1882**	https://github.com/thorsten/phpmyfaq/commit/49db615c300ae0f87795f20570f6f5bdccb1d2f2, https://huntr.dev/bounties/8ab09a1c-cfd5-4ce0-aae3-d33c93318957	A-PHP-PHPM-200423/502

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	05-Apr-2023	5.4	Improper Access Control in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1883**	https://github.com/thorsten/phpmyfaq/commit/db77df8881787669873985 97d4f153831c62a503, https://huntr.dev/bounties/2f1e417d-cf64-4cfb-954b-3a9cb2f38191	A-PHP-PHPM-200423/503
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1885**	https://github.com/thorsten/phpmyfaq/commit/fecc803ab9c3e82718c4bcea7fe919d7a22ec024, https://huntr.dev/bounties/bce84c02-abb2-474f-a67b-1468c9dcabb8	A-PHP-PHPM-200423/504
N/A	05-Apr-2023	4.3	Business Logic Errors in GitHub repository thorsten/phpmyfaq prior to 3.1.12. **CVE ID : CVE-2023-1887**	https://github.com/thorsten/phpmyfaq/commit/400d9cd988d3287515c56b2ad6343026966f1a89, https://huntr.dev/bounties/e4a58835-96b5-412c-a17e-3ceed30231e1	A-PHP-PHPM-200423/505

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Pimcore					
Product: perspective_editor					
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Pimcore Perspective Editor provides an editor for Pimcore that allows users to add/remove/edit custom views and perspectives. This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie or redirect users to other malicious sites. Version 1.5.1 has a patch. As a workaround, one may apply the patch manually. **CVE ID : CVE-2023-28850**	https://github.com/pimcore/perspective-editor/pull/121.patch, https://huntr.dev/bounties/5529f51e-e40f-46f1-887b-c9dbebab4f06/, https://github.com/pimcore/perspective-editor/security/advisories/GHSA-fq8q-55v3-2986	A-PIM-PERS-200423/506
Vendor: pinpoint					
Product: pinpoint_booking_system					
Affected Version(s): * Up to (excluding) 2.9.9.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PINPOINT.WORLD Pinpoint Booking System plugin <= 2.9.9.2.8 versions. **CVE ID : CVE-2023-25062**	N/A	A-PIN-PINP-200423/507
Vendor: piwebsolution					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: product_enquiry_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.2.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in PI Websolution Product Enquiry for WooCommerce, WooCommerce product catalog plugin <= 2.2.12 versions. **CVE ID : CVE-2023-29170**	N/A	A-PIW-PROD-200423/508
Product: product_page_shipping_calculator_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.3.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in PI Websolution Product page shipping calculator for WooCommerce plugin <= 1.3.20 versions. **CVE ID : CVE-2023-29094**	N/A	A-PIW-PROD-200423/509
Vendor: plugin					
Product: yourchannel					
Affected Version(s): * Up to (including) 1.2.3					
Missing Authorization	05-Apr-2023	6.5	The YourChannel plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check when resetting	https://plugins.trac.wordpress.org/browser/yourchannel/trunk/YourChannel.php?rev=2844975#L772	A-PLU-YOUR-200423/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin settings via the yrc_nuke GET parameter in versions up to, and including, 1.2.3. This makes it possible for unauthenticated attackers to delete YouTube channels from the plugin. **CVE ID : CVE-2023-1865**		
Missing Authorization	05-Apr-2023	5.3	The YourChannel plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check when clearing the plugin cache via the yrc_clear_cache GET parameter in versions up to, and including, 1.2.3. This makes it possible for unauthenticated attackers to clear the plugin's cache. **CVE ID : CVE-2023-1868**	https://plugins.trac.wordpress.org/browser/yourchannel/trunk/YourChannel.php?rev=2844975#L768	A-PLU-YOUR-200423/511
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	4.8	The YourChannel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 1.2.3 due to insufficient input sanitization and output escaping. This makes it possible for	N/A	A-PLU-YOUR-200423/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attackers, with administrative-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-1869**		
Cross-Site Request Forgery (CSRF)	05-Apr-2023	4.3	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the clearKeys function. This makes it possible for unauthenticated attackers to reset the plugin's channel settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1866**	https://plugins.trac.wordpress.org/browser/yourchannel/trunk/YourChannel.php?rev=2844975#L107	A-PLU-YOUR-200423/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	05-Apr-2023	4.3	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the save function. This makes it possible for unauthenticated attackers to change the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1867**	https://plugins.trac.wordpress.org/browser/yourchannel/trunk/YourChannel.php?rev=2844975#L426	A-PLU-YOUR-200423/514
Cross-Site Request Forgery (CSRF)	05-Apr-2023	4.3	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the saveLang function. This makes it possible for unauthenticated attackers to change the plugin's quick language translation settings via a forged request granted they	https://plugins.trac.wordpress.org/browser/yourchannel/trunk/YourChannel.php?rev=2844975#L498	A-PLU-YOUR-200423/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1870**		
Cross-Site Request Forgery (CSRF)	05-Apr-2023	4.3	The YourChannel plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the deleteLang function. This makes it possible for unauthenticated attackers to reset the plugin's quick language translation settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1871**	https://plugins.trac.wordpress.org/browser/yourchannel/trunk/YourChannel.php?rev=2844975#L505	A-PLU-YOUR-200423/516
Vendor: podlove					
Product: podlove_podcast_publisher					
Affected Version(s): * Up to (including) 3.8.2					
Improper Neutralization of Input During Web Page	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Podlove Podlove Podcast Publisher	N/A	A-POD-PODL-200423/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			plugin <= 3.8.2 versions. **CVE ID : CVE-2023-25046**		
Vendor: police_crime_record_management_system_project					
Product: police_crime_record_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Apr-2023	9.8	A vulnerability was found in SourceCodester Police Crime Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file /officer/assigncase.php of the component GET Parameter Handler. The manipulation of the argument caseid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-224745 was assigned to this vulnerability. **CVE ID : CVE-2023-1793**	N/A	A-POL-POLI-200423/518
Improper Neutralization of Input During Web Page	02-Apr-2023	6.1	A vulnerability was found in SourceCodester Police Crime Record Management System 1.0. It has been	N/A	A-POL-POLI-200423/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			declared as problematic. This vulnerability affects unknown code of the file /admin/casedetails.php of the component GET Parameter Handler. The manipulation of the argument id with the input "><script>alert(233)</script> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-224746 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1794**		
Vendor: polymc					
Product: polymc					
Affected Version(s): * Up to (excluding) 5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Apr-2023	7.1	PolyMC Launcher <= 1.4.3 is vulnerable to Directory Traversal. A mrpack file can be maliciously crafted to create arbitrary files outside of the installation directory. **CVE ID : CVE-2023-25305**	https://github.com/PolyMC/PolyMC/security/advisories/GHSA-3rfr-g9g9-7gx2	A-POL-POLY-200423/520
Vendor: Powerdns					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: recursor					
Affected Version(s): * Up to (excluding) 4.6.6					
N/A	04-Apr-2023	5.3	Denial of service vulnerability in PowerDNS Recursor allows authoritative servers to be marked unavailable.This issue affects Recursor: through 4.6.5, through 4.7.4 , through 4.8.3. **CVE ID : CVE-2023-26437**	https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2023-02.html	A-POW-RECU-200423/521
Affected Version(s): From (including) 4.7.0 Up to (excluding) 4.7.5					
N/A	04-Apr-2023	5.3	Denial of service vulnerability in PowerDNS Recursor allows authoritative servers to be marked unavailable.This issue affects Recursor: through 4.6.5, through 4.7.4 , through 4.8.3. **CVE ID : CVE-2023-26437**	https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2023-02.html	A-POW-RECU-200423/522
Affected Version(s): From (including) 4.8.0 Up to (excluding) 4.8.4					
N/A	04-Apr-2023	5.3	Denial of service vulnerability in PowerDNS Recursor allows authoritative servers to be marked unavailable.This issue affects Recursor: through	https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2023-02.html	A-POW-RECU-200423/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.6.5, through 4.7.4 , through 4.8.3. **CVE ID : CVE-2023-26437**		
Vendor: Progress					
Product: sitefinity					
Affected Version(s): From (including) 13.3 Up to (excluding) 13.3.7646					
Unrestricted Upload of File with Dangerous Type	10-Apr-2023	9.8	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potentially dangerous file upload through the SharePoint connector. **CVE ID : CVE-2023-29375**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/524
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potential XSS by privileged users in	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sitefinity to media libraries. **CVE ID : CVE-2023-29376**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.7736					
Unrestricted Upload of File with Dangerous Type	10-Apr-2023	9.8	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potentially dangerous file upload through the SharePoint connector. **CVE ID : CVE-2023-29375**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/526
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potential XSS by privileged users in Sitefinity to media libraries. **CVE ID : CVE-2023-29376**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/527
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1.7826					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	10-Apr-2023	9.8	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potentially dangerous file upload through the SharePoint connector. **CVE ID : CVE-2023-29375**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/528
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potential XSS by privileged users in Sitefinity to media libraries. **CVE ID : CVE-2023-29376**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/529
Affected Version(s): From (including) 14.2 Up to (excluding) 14.2.7930					
Unrestricted Upload of File with Dangerous Type	10-Apr-2023	9.8	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736,	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-	A-PRO-SITE-200423/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potentially dangerous file upload through the SharePoint connector. **CVE ID : CVE-2023-29375**	Addressing-Security-Vulnerabilities-April-2023	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potential XSS by privileged users in Sitefinity to media libraries. **CVE ID : CVE-2023-29376**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/531
Affected Version(s): From (including) 14.3 Up to (excluding) 14.3.8026					
Unrestricted Upload of File with Dangerous Type	10-Apr-2023	9.8	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potentially	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dangerous file upload through the SharePoint connector. **CVE ID : CVE-2023-29375**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	5.4	An issue was discovered in Progress Sitefinity 13.3 before 13.3.7647, 14.0 before 14.0.7736, 14.1 before 14.1.7826, 14.2 before 14.2.7930, and 14.3 before 14.3.8025. There is potential XSS by privileged users in Sitefinity to media libraries. **CVE ID : CVE-2023-29376**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerabilities-April-2023	A-PRO-SITE-200423/533
Vendor: prolizyazilim					
Product: student_affairs_information_system					
Affected Version(s): * Up to (excluding) 23.04.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proliz OBS allows Stored XSS for an authenticated user.This issue affects OBS: before 23.04.01. **CVE ID : CVE-2023-1726**	N/A	A-PRO-STUD-200423/534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: properfraction					
Product: profilepress					
Affected Version(s): * Up to (excluding) 4.5.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in ProfilePress Membership Team ProfilePress plugin <= 4.5.3 versions. **CVE ID : CVE-2023-23996**	N/A	A-PRO-PROF-200423/535
Vendor: quantumcloud					
Product: conversational_forms_for_chatbot					
Affected Version(s): * Up to (excluding) 1.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in QuantumCloud Conversational Forms for ChatBot plugin <= 1.1.6 versions. **CVE ID : CVE-2023-23981**	N/A	A-QUA-CONV-200423/536
Vendor: radiustheme					
Product: portfolio					
Affected Version(s): * Up to (excluding) 2.8.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in RadiusTheme Portfolio – WordPress Portfolio plugin <= 2.8.10 versions.	N/A	A-RAD-PORT-200423/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23685		
Vendor: readium					
Product: readium-js					
Affected Version(s): 0.32.0					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	An arbitrary file upload vulnerability in readium-js v0.32.0 allows attackers to execute arbitrary code via uploading a crafted EPUB file. **CVE ID : CVE-2023-24720**	N/A	A-REA-READ-200423/538
Vendor: redpanda					
Product: redpanda					
Affected Version(s): * Up to (excluding) 23.1.2					
N/A	08-Apr-2023	4.3	rpk in Redpanda before 23.1.2 mishandles the redpanda.rpc_server_tls field, leading to (for example) situations in which there is a data type mismatch that cannot be automatically fixed by rpk, and instead a user must reconfigure (while a cluster is turned off) in order to have TLS on broker RPC ports. NOTE: the fix was also backported to the 22.2 and 22.3 branches. **CVE ID : CVE-2023-30450**	https://github.com/redpanda-data/redpanda/commit/a839056381ea7cd71e68495854e388daf7a08ba7, https://github.com/redpanda-data/redpanda/commit/58795aa07e88e0a63cebf4e1d9fcc717ceef0557, https://github.com/redpanda-data/redpanda/pull/7719	A-RED-REDP-200423/539

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: robogallery					
Product: robo_gallery					
Affected Version(s): * Up to (excluding) 3.2.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	5.4	Auth. (contributor+) Stored Cross-site Scripting (XSS) vulnerability in RoboSoft Photo Gallery, Images, Slider in Rbs Image Gallery plugin <= 3.2.12 versions. **CVE ID : CVE-2023-27620**	N/A	A-ROB-ROBO-200423/540
Vendor: ruoyi					
Product: ruoyi					
Affected Version(s): * Up to (including) 4.7.6					
Download of Code Without Integrity Check	02-Apr-2023	7.5	An arbitrary file download vulnerability in the background management module of RuoYi v4.7.6 and below allows attackers to download arbitrary files in the server. **CVE ID : CVE-2023-27025**	N/A	A-RUO-RUOY-200423/541
Vendor: safe-eval_project					
Product: safe-eval					
Affected Version(s): * Up to (including) 0.4.1					
Improperly Controlled Modification of Object Prototype Attributes	11-Apr-2023	10	All versions of the package safe-eval are vulnerable to Prototype Pollution via the safeEval function, due to improper	N/A	A-SAF-SAFE-200423/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Prototype Pollution')			sanitization of its parameter content. **CVE ID : CVE-2023-26121**		
Vendor: sagemath					
Product: flintqs					
Affected Version(s): 1.0					
N/A	06-Apr-2023	5.5	SageMath FlintQS 1.0 relies on pathnames under TMPDIR (typically world-writable), which (for example) allows a local user to overwrite files with the privileges of a different user (who is running FlintQS). **CVE ID : CVE-2023-29465**	https://github.com/sagemath/sage/pull/35419	A-SAG-FLIN-200423/543
Vendor: saleswonder					
Product: webinar_ignition					
Affected Version(s): * Up to (including) 2.14.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Saleswonder.Biz Webinar ignition plugin <= 2.14.2 versions. **CVE ID : CVE-2023-25023**	N/A	A-SAL-WEBI-200423/544
Vendor: sales_tracker_management_system_project					
Product: sales_tracker_management_system					
Affected Version(s): 1.0					
N/A	10-Apr-2023	7.5	An issue found in Sales Tracker Management System	N/A	A-SAL-SALE-200423/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v.1.0 allows a remote attacker to access sensitive information via sales.php component of the admin/reports endpoint. **CVE ID : CVE-2023-26774**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	6.1	Cross Site Scripting vulnerability found in Sales Tracker Management System v.1.0 allows a remote attacker to gain privileges via the product list function in the Master.php file. **CVE ID : CVE-2023-26773**	N/A	A-SAL-SALE-200423/546
Vendor: Samba					
Product: samba					
Affected Version(s): From (including) 4.8.0 Up to (excluding) 4.8.4					
Cleartext Storage of Sensitive Information	03-Apr-2023	6.5	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure vi LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC. **CVE ID : CVE-2023-0614**	https://www.samba.org/samba/security/CVE-2023-0614.html, https://security.netapp.com/advisory/ntap-20230406-0007/	A-SAM-SAMB-200423/547
Affected Version(s): 4.18.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	03-Apr-2023	5.9	The Samba AD DC administration tool, when operating against a remote LDAP server, will by default send new or reset passwords over a signed-only connection. **CVE ID : CVE-2023-0922**	https://www.samba.org/samba/security/CVE-2023-0922.html, https://security.netapp.com/advisory/ntap-20230406-0007/	A-SAM-SAMB-200423/548
Incorrect Permission Assignment for Critical Resource	03-Apr-2023	4.3	A flaw was found in Samba. An incomplete access check on dnsHostName allows authenticated but otherwise unprivileged users to delete this attribute from any object in the directory. **CVE ID : CVE-2023-0225**	https://www.samba.org/samba/security/CVE-2023-0225.html, https://security.netapp.com/advisory/ntap-20230406-0007/	A-SAM-SAMB-200423/549
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.16.10					
Cleartext Transmission of Sensitive Information	03-Apr-2023	5.9	The Samba AD DC administration tool, when operating against a remote LDAP server, will by default send new or reset passwords over a signed-only connection. **CVE ID : CVE-2023-0922**	https://www.samba.org/samba/security/CVE-2023-0922.html, https://security.netapp.com/advisory/ntap-20230406-0007/	A-SAM-SAMB-200423/550
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.6.16					
Cleartext Storage of Sensitive	03-Apr-2023	6.5	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential	https://www.samba.org/samba/security/CVE-2023-	A-SAM-SAMB-200423/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			attribute disclosure vi LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC. **CVE ID : CVE-2023-0614**	0614.html, https://security.netapp.com/advisory/ntap-20230406-0007/	
Affected Version(s): From (including) 4.17.0 Up to (excluding) 4.17.7					
Cleartext Transmission of Sensitive Information	03-Apr-2023	5.9	The Samba AD DC administration tool, when operating against a remote LDAP server, will by default send new or reset passwords over a signed-only connection. **CVE ID : CVE-2023-0922**	https://www.samba.org/samba/security/CVE-2023-0922.html, https://security.netapp.com/advisory/ntap-20230406-0007/	A-SAM-SAMB-200423/552
Incorrect Permission Assignment for Critical Resource	03-Apr-2023	4.3	A flaw was found in Samba. An incomplete access check on dnsHostName allows authenticated but otherwise unprivileged users to delete this attribute from any object in the directory. **CVE ID : CVE-2023-0225**	https://www.samba.org/samba/security/CVE-2023-0225.html, https://security.netapp.com/advisory/ntap-20230406-0007/	A-SAM-SAMB-200423/553
Affected Version(s): From (including) 4.7.0 Up to (excluding) 4.7.9					
Cleartext Storage of Sensitive Information	03-Apr-2023	6.5	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure	https://www.samba.org/samba/security/CVE-2023-0614.html,	A-SAM-SAMB-200423/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vi LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC. **CVE ID : CVE-2023-0614**	https://security.netapp.com/advisory/ntap-20230406-0007/	
Affected Version(s): From (including) 4.9.0 Up to (excluding) 4.9.4					
Cleartext Storage of Sensitive Information	03-Apr-2023	6.5	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure vi LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC. **CVE ID : CVE-2023-0614**	https://www.samba.org/samba/security/CVE-2023-0614.html, https://security.netapp.com/advisory/ntap-20230406-0007/	A-SAM-SAMB-200423/555
Vendor: SAP					
Product: abap_platform					
Affected Version(s): 75c					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-200423/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29110**		
Affected Version(s): 75d					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-200423/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			integrity of the application. **CVE ID : CVE-2023-29110**		
Affected Version(s): 75e					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29110**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-ABAP-200423/558
Product: application_interface					
Affected Version(s): 600					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Monitoring) - versions 600, 700, allows an authorized attacker to input links or headings with custom CSS classes into a comment. The comment will render links and custom CSS classes as HTML objects. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29112**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-APPL-200423/559
Affected Version(s): 700					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Monitoring) - versions 600, 700, allows an authorized attacker to input links or headings with custom CSS classes into a comment. The comment will render links and custom CSS classes as HTML objects. After successful exploitations, an	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-APPL-200423/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29112**		
Product: application_interface_framework					
Affected Version(s): 755					
N/A	11-Apr-2023	4.3	The SAP AIF (ODATA service) - versions 755, 756, discloses more detailed information than is required. An authorized attacker can use the collected information possibly to exploit the component. As a result, an attacker can cause a low impact on the confidentiality of the application. **CVE ID : CVE-2023-29111**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-APPL-200423/561
Affected Version(s): 756					
N/A	11-Apr-2023	4.3	The SAP AIF (ODATA service) - versions 755, 756, discloses more detailed information than is required. An authorized attacker can use the collected	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-APPL-200423/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information possibly to exploit the component. As a result, an attacker can cause a low impact on the confidentiality of the application. **CVE ID : CVE-2023-29111**		
Affected Version(s): aif_703					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-APPL-200423/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29110		
Affected Version(s): aifx_702					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29110**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-APPL-200423/564
Product: basis					
Affected Version(s): 755					
Improper Neutralization of Input During Web Page	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-BASI-200423/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29110**	c68f7e60039b.html	
Affected Version(s): 756					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BASI-200423/566

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29110**		
Product: businessobjects_business_intelligence					
Affected Version(s): 420					
N/A	11-Apr-2023	9.8	An attacker with basic privileges in SAP BusinessObjects Business Intelligence Platform (Promotion Management) - versions 420, 430, can get access to lcmbiar file and further decrypt the file. After this attacker can gain access to BI user's passwords and depending on the privileges of the BI user, the attacker can perform operations that can completely compromise the application. **CVE ID : CVE-2023-28765**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-200423/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 430					
N/A	11-Apr-2023	9.8	An attacker with basic privileges in SAP BusinessObjects Business Intelligence Platform (Promotion Management) - versions 420, 430, can get access to lcmbiar file and further decrypt the file. After this attacker can gain access to BI user's passwords and depending on the privileges of the BI user, the attacker can perform operations that can completely compromise the application. **CVE ID : CVE-2023-28765**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-200423/568
Product: customer_relationship_management					
Affected Version(s): 700					
Improper Control of Generation of Code ('Code Injection')	11-Apr-2023	6.3	In SAP CRM - versions 700, 701, 702, 712, 713, an attacker who is authenticated with a non-administrative role and a common remote execution authorization can use a vulnerable interface to execute an application function to perform actions which they	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-200423/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would not normally be permitted to perform. Depending on the function executed, the attack can can have limited impact on confidentiality and integrity of non-critical user or application data and application availability. **CVE ID : CVE-2023-27897**		
Affected Version(s): 701					
Improper Control of Generation of Code ('Code Injection')	11-Apr-2023	6.3	In SAP CRM - versions 700, 701, 702, 712, 713, an attacker who is authenticated with a non-administrative role and a common remote execution authorization can use a vulnerable interface to execute an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can can have limited impact on confidentiality and integrity of non-critical user or	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-200423/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application data and application availability. **CVE ID : CVE-2023-27897**		
Affected Version(s): 702					
Improper Control of Generation of Code ('Code Injection')	11-Apr-2023	6.3	In SAP CRM - versions 700, 701, 702, 712, 713, an attacker who is authenticated with a non-administrative role and a common remote execution authorization can use a vulnerable interface to execute an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can can have limited impact on confidentiality and integrity of non-critical user or application data and application availability. **CVE ID : CVE-2023-27897**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-200423/571
Affected Version(s): 712					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	11-Apr-2023	6.3	In SAP CRM - versions 700, 701, 702, 712, 713, an attacker who is authenticated with a non-administrative role and a common remote execution authorization can use a vulnerable interface to execute an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can can have limited impact on confidentiality and integrity of non-critical user or application data and application availability. **CVE ID : CVE-2023-27897**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-200423/572
Affected Version(s): 713					
Improper Control of Generation of Code ('Code Injection')	11-Apr-2023	6.3	In SAP CRM - versions 700, 701, 702, 712, 713, an attacker who is authenticated with a non-administrative role and a common remote execution authorization can use a vulnerable	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-CUST-200423/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface to execute an application function to perform actions which they would not normally be permitted to perform. Depending on the function executed, the attack can can have limited impact on confidentiality and integrity of non-critical user or application data and application availability. **CVE ID : CVE-2023-27897**		
Product: diagnostics_agent					
Affected Version(s): 720					
Missing Authentication for Critical Function	11-Apr-2023	8.1	Due to missing authentication and insufficient input validation, the OSCommand Bridge of SAP Diagnostics Agent - version 720, allows an attacker with deep knowledge of the system to execute scripts on all connected Diagnostics Agents. On successful exploitation, the attacker can completely compromise	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-DIAG-200423/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity and availability of the system. **CVE ID : CVE-2023-27267**		
Product: hcm_fiori_app_my_forms					
Affected Version(s): 605					
Missing Authorization	11-Apr-2023	4.3	SAP HCM Fiori App My Forms (Fiori 2.0) - version 605, does not perform necessary authorization checks for an authenticated user exposing the restricted header data. **CVE ID : CVE-2023-1903**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-HCM_-200423/575
Product: landscape_management					
Affected Version(s): 3.0					
Exposure of Resource to Wrong Sphere	11-Apr-2023	8.7	An information disclosure vulnerability exists in SAP Landscape Management - version 3.0, enterprise edition. It allows an authenticated SAP Landscape Management user to obtain privileged access to other systems making	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-LAND-200423/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			those other systems vulnerable to information disclosure and modification.The disclosed information is for Diagnostics Agent Connection via Java SCS Message Server of an SAP Solution Manager system and can only be accessed by authenticated SAP Landscape Management users, but they can escalate their privileges to the SAP Solution Manager system. **CVE ID : CVE-2023-26458**		
Product: netweaver_application_server_abap					
Affected Version(s): 755					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the network without any user interaction. **CVE ID : CVE-2023-28763**		
Affected Version(s): 756					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/578
Affected Version(s): 740					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**		
Affected Version(s): 750					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/580
Affected Version(s): 751					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-	A-SAP-NETW-200423/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**	c68f7e60039b.html	
Affected Version(s): 752					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/582
Affected Version(s): 753					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/583
Affected Version(s): 754					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction.	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28763		
Affected Version(s): 757					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/585
Affected Version(s): 791					
N/A	11-Apr-2023	6.5	SAP NetWeaver AS for ABAP and ABAP Platform - versions 740, 750, 751, 752, 753, 754, 755, 756, 757, 791, allows an attacker authenticated as a non-administrative user to craft a request with certain parameters which can consume the server's resources	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sufficiently to make it unavailable over the network without any user interaction. **CVE ID : CVE-2023-28763**		
Product: netweaver_as_java_for_deploy_service					
Affected Version(s): 7.5					
Missing Authentication for Critical Function	11-Apr-2023	5.3	SAP NetWeaver AS Java for Deploy Service - version 7.5, does not perform any access control checks for functionalities that require user identity enabling an unauthenticated attacker to attach to an open interface and make use of an open naming and directory API to access a service which will enable them to access but not modify server settings and data with no effect on availability and integrity. **CVE ID : CVE-2023-24527**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/587
Product: netweaver_enterprise_portal					
Affected Version(s): 7.50					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	11-Apr-2023	6.5	In SAP NetWeaver Enterprise Portal - version 7.50, an unauthenticated attacker can attach to an open interface and make use of an open API to access a service which will enable them to access or modify server settings and data, leading to limited impact on confidentiality and integrity. **CVE ID : CVE-2023-28761**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-NETW-200423/588
Product: s4core					
Affected Version(s): 100					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4CO-200423/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29110**		
Affected Version(s): 101					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	The SAP Application Interface (Message Dashboard) - versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E, application allows the usage HTML tags. An authorized attacker can use some of the basic HTML codes such as heading, basic formatting and lists, then an attacker can inject images from the foreign domains. After successful exploitations, an attacker can cause limited impact on the confidentiality and integrity of the application. **CVE ID : CVE-2023-29110**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-S4CO-200423/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: SAS					
Product: web_administration_interface					
Affected Version(s): 9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	A stored cross site scripting (XSS) vulnerability was discovered in the user management module of the SAS 9.4 Admin Console, due to insufficient validation and sanitization of data input into the user creation and editing form fields. The product name is SAS Web Administration interface (SASAdmin). For the product release, the reported version is 9.4_M2 and the fixed version is 9.4_M3. For the SAS release, the reported version is 9.4 TS1M2 and the fixed version is 9.4 TS1M3. **CVE ID : CVE-2023-24724**	https://support.sas.com/kb/55/539.html	A-SAS-WEB_-200423/591
Vendor: save_your_carts_and_buy_later_or_send_it_project					
Product: save_your_carts_and_buy_later_or_send_it					
Affected Version(s): * Up to (including) 1.0.3					
Improper Neutralization of Special Elements used in an SQL	10-Apr-2023	8.8	SQL injection vulnerability found in PrestaShop Igbudget v.1.0.3 and before allow a remote attacker to gain privileges via	https://friends-of-presta.github.io/security-advisories/modules/2023/0	A-SAV-SAVE-200423/592

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			the LgBudgetBudgetModuleFrontController::displayAjaxGenerateBudget component. **CVE ID : CVE-2023-26860**	4/04/lgbudget.html	
Vendor: silverwaregames					
Product: silverwaregames					
Affected Version(s): * Up to (excluding) 1.2.19					
Exposure of Resource to Wrong Sphere	10-Apr-2023	4.3	SilverwareGames.io versions before 1.2.19 allow users with access to the game upload panel to edit download links for games uploaded by other developers. This has been fixed in version 1.2.19. **CVE ID : CVE-2023-29192**	N/A	A-SIL-SILV-200423/593
Vendor: simple_and_beautiful_shopping_cart_system_project					
Product: simple_and_beautiful_shopping_cart_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Apr-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Simple and Beautiful Shopping Cart System 1.0. This issue affects some unknown processing of the file login.php. The manipulation of the argument username/password leads to sql injection.	N/A	A-SIM-SIMP-200423/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225317 was assigned to this vulnerability. **CVE ID : CVE-2023-1941**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Apr-2023	9.1	A vulnerability classified as critical was found in SourceCodester Simple and Beautiful Shopping Cart System 1.0. This vulnerability affects unknown code of the file delete_user_query.php. The manipulation of the argument user_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-225316. **CVE ID : CVE-2023-1940**	N/A	A-SIM-SIMP-200423/595
Vendor: simple_guestbook_management_system_project					
Product: simple_guestbook_management_system					
Affected Version(s): 1.0					
Improper Neutralization of	06-Apr-2023	6.1	Sourcecodester Simple Guestbook Management System	http://sourcecodester.com	A-SIM-SIMP-200423/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			version 1 is vulnerable to Cross Site Scripting (XSS) via Name, Referrer, Location, and Comments. **CVE ID : CVE-2023-22985**		
Vendor: simple_mobile_comparison_website_project					
Product: simple_mobile_comparison_website					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Apr-2023	9.8	A vulnerability was found in SourceCodester Simple Mobile Comparison Website 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/fields/manage_field.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-224744. **CVE ID : CVE-2023-1792**	N/A	A-SIM-SIMP-200423/597
Improper Neutralization of	06-Apr-2023	9.8	A vulnerability was found in SourceCodester	N/A	A-SIM-SIMP-200423/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Simple Mobile Comparison Website 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/categories/view_category.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225150 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1908**		
Vendor: simple_staff_list_project					
Product: simple_staff_list					
Affected Version(s): * Up to (excluding) 2.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Brett Shumaker Simple Staff List plugin <= 2.2.2 versions. **CVE ID : CVE-2023-23686**	N/A	A-SIM-SIMP-200423/599
Vendor: simple_task_allocation_system_project					
Product: simple_task_allocation_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Apr-2023	9.8	A vulnerability has been found in SourceCodester Simple Task Allocation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-224743. **CVE ID : CVE-2023-1791**	N/A	A-SIM-SIMP-200423/600
N/A	01-Apr-2023	7.5	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Task Allocation System 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument page leads to information disclosure. It is possible to launch the attack remotely. The exploit has been	N/A	A-SIM-SIMP-200423/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier of this vulnerability is VDB-224724. **CVE ID : CVE-2023-1790**		
Vendor: siteproxy_project					
Product: siteproxy					
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Apr-2023	7.5	siteproxy v1.0 was discovered to contain a path traversal vulnerability via the component index.js. **CVE ID : CVE-2023-26820**	N/A	A-SIT-SITE-200423/602
Vendor: snapcreek					
Product: ezp_coming_soon_page					
Affected Version(s): * Up to (including) 1.0.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Snap Creek Software EZP Coming Soon Page plugin <= 1.0.7.3 versions. **CVE ID : CVE-2023-24398**	N/A	A-SNA-EZP_-200423/603
Vendor: solidres					
Product: solidres					
Affected Version(s): * Up to (including) 0.9.4					
Improper Neutralization of Input	03-Apr-2023	6.1	The Solidres WordPress plugin through 0.9.4 does not sanitise and	N/A	A-SOL-SOLI-200423/604

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			escape numerous parameter before outputting them back in pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-1377**		
Vendor: Sophos					
Product: web_appliance					
Affected Version(s): * Up to (excluding) 4.3.10.4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2023	9.8	A pre-auth command injection vulnerability in the warn-proceed handler of Sophos Web Appliance older than version 4.3.10.4 allows execution of arbitrary code. **CVE ID : CVE-2023-1671**	https://www.sophos.com/en-us/security-advisories/sophos-sa-20230404-swa-rce	A-SOP-WEB_-200423/605
Vendor: streamweasels					
Product: twitch_player					
Affected Version(s): * Up to (excluding) 2.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in StreamWeasels Twitch Player plugin <= 2.1.0 versions. **CVE ID : CVE-2023-25464**	N/A	A-STR-TWIT-200423/606
Vendor: stylishcostcalculator					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: stylish_cost_calculator					
Affected Version(s): * Up to (including) 7.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	6.1	The stylish-cost-calculator-premium WordPress plugin before 7.9.0 does not sanitise and escape a parameter before outputting it back in the page, leading to a Stored Cross-Site Scripting which could be used against admins when viewing submissions submitted through the Email Quote Form. **CVE ID : CVE-2023-0983**	N/A	A-STY-STYL-200423/607
Vendor: survey_application_system_project					
Product: survey_application_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	A vulnerability was found in SourceCodester Survey Application System 1.0 and classified as problematic. This issue affects some unknown processing of the component Add New Handler. The manipulation of the argument Title with the input <script>prompt(document.domain)</script> leads to cross site scripting. The attack may be	N/A	A-SUR-SURV-200423/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-225329 was assigned to this vulnerability. **CVE ID : CVE-2023-1946**		
Vendor: svelte					
Product: sveltekit					
Affected Version(s): * Up to (excluding) 1.15.1					
Cross-Site Request Forgery (CSRF)	04-Apr-2023	8.8	SvelteKit is a web development framework. The SvelteKit framework offers developers an option to create simple REST APIs. This is done by defining a `+server.js` file, containing endpoint handlers for different HTTP methods. SvelteKit provides out-of-the-box cross-site request forgery (CSRF) protection to its users. While the implementation does a sufficient job in mitigating common CSRF attacks, prior to version 1.15.1, the protection can be bypassed by simply specifying a different `Content-Type` header value. If	https://github.com/sveltejs/kit/releases/tag/%40sveltejs%2Fkit%401.15.1, https://github.com/sveltejs/kit/commit/bb2253d51d00aba2e4353952d4fb0dcde6c77123, https://github.com/sveltejs/kit/security/advisories/GHSA-5p75-vc5g-8rv2	A-SVE-SVEL-200423/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			abused, this issue will allow malicious requests to be submitted from third-party domains, which can allow execution of operations within the context of the victim's session, and in extreme scenarios can lead to unauthorized access to users' accounts. SvelteKit 1.15.1 updates the `is_form_content_type` function call in the CSRF protection logic to include `text/plain`. As additional hardening of the CSRF protection mechanism against potential method overrides, SvelteKit 1.15.1 is now performing validation on `PUT`, `PATCH` and `DELETE` methods as well. This latter hardening is only needed to protect users who have put in some sort of `?_method= override` feature themselves in their `handle` hook, so that the request that resolve sees could be `PUT`/`PATCH`/`DEL		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ETE` when the browser issues a `POST` request. **CVE ID : CVE-2023-29003**		
Affected Version(s): * Up to (excluding) 1.15.2					
Cross-Site Request Forgery (CSRF)	06-Apr-2023	8.8	The SvelteKit framework offers developers an option to create simple REST APIs. This is done by defining a `+server.js` file, containing endpoint handlers for different HTTP methods. SvelteKit provides out-of-the-box cross-site request forgery (CSRF) protection to its users. The protection is implemented at `kit/src/runtime/server/respond.js`. While the implementation does a sufficient job of mitigating common CSRF attacks, the protection can be bypassed in versions prior to 1.15.2 by simply specifying an upper-cased `Content-Type` header value. The browser will not send uppercase characters, but this check does not block all expected CORS	https://github.com/sveltejs/kit/commit/ba436c6685e751d968a960fbda65f24cf7a82e9f, https://github.com/sveltejs/kit/security/advisories/GHSA-gv7g-x59x-wf8f	A-SVE-SVEL-200423/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests. If abused, this issue will allow malicious requests to be submitted from third-party domains, which can allow execution of operations within the context of the victim's session, and in extreme scenarios can lead to unauthorized access to users’ accounts. This may lead to all POST operations requiring authentication being allowed in the following cases: If the target site sets `SameSite=None` on its auth cookie and the user visits a malicious site in a Chromium-based browser; if the target site doesn't set the `SameSite` attribute explicitly and the user visits a malicious site with Firefox/Safari with tracking protections turned off; and/or if the user is visiting a malicious site with a very outdated browser. SvelteKit 1.15.2 contains a patch for this issue. It is also recommended to explicitly set		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`SameSite` to a value other than `None` on authentication cookies especially if the upgrade cannot be done in a timely manner. **CVE ID : CVE-2023-29008**		
Vendor: Swftools					
Product: swftools					
Affected Version(s): 0.9.2					
Use After Free	04-Apr-2023	7.8	SWFTools v0.9.2 was discovered to contain a stack-use-after-scope in the swf_ReadSWF2 function in lib/rfxswf.c. **CVE ID : CVE-2023-26991**	N/A	A-SWF-SWFT-200423/611
Vendor: taogogo					
Product: taocms					
Affected Version(s): 3.0.2					
Improper Control of Generation of Code ('Code Injection')	07-Apr-2023	9.8	A vulnerability was found in taoCMS 3.0.2. It has been classified as critical. Affected is an unknown function of the file /admin/admin.php. The manipulation leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-225330 is	N/A	A-TAO-TAOC-200423/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the identifier assigned to this vulnerability. **CVE ID : CVE-2023-1947**		
Vendor: Tcpdump					
Product: tcpdump					
Affected Version(s): 4.99.3					
Out-of-bounds Write	07-Apr-2023	6.5	The SMB protocol decoder in tcpdump version 4.99.3 can perform an out-of-bounds write when decoding a crafted network packet. **CVE ID : CVE-2023-1801**	https://github.com/the-tcpdump-group/tcpdump/commit/03c037bbd75588beba3ee09f26d17783d21e30bc, https://github.com/the-tcpdump-group/tcpdump/commit/7578e1c04ee280dda50c4c2813e7d55f539c6501	A-TCP-TCPD-200423/613
Vendor: teacms_project					
Product: teacms					
Affected Version(s): 2.3.3					
Improper Authentication	04-Apr-2023	7.2	An unauthorized access issue found in XiaoBingby TeaCMS 2.3.3 allows attackers to escalate privileges via the id and keywords parameter(s). **CVE ID : CVE-2023-27091**	N/A	A-TEA-TEAC-200423/614
Vendor: teclib-edition					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: fields					
Affected Version(s): * Up to (excluding) 1.13.1					
Improper Privilege Management	05-Apr-2023	6.5	Fields is a GLPI plugin that allows users to add custom fields on GLPI items forms. Prior to versions 1.13.1 and 1.20.4, lack of access control check allows any authenticated user to write data to any fields container, including those to which they have no configured access. Versions 1.13.1 and 1.20.4 contain a patch for this issue. **CVE ID : CVE-2023-28855**	https://github.com/pluginsGLPI/fields/security/advisories/GHSA-52vv-hm4x-8584, https://github.com/pluginsGLPI/fields/commit/784260be7db185bb1e7d66b299997238c4c0205d	A-TEC-FIEL-200423/615
Affected Version(s): From (including) 1.20.0 Up to (excluding) 1.20.4					
Improper Privilege Management	05-Apr-2023	6.5	Fields is a GLPI plugin that allows users to add custom fields on GLPI items forms. Prior to versions 1.13.1 and 1.20.4, lack of access control check allows any authenticated user to write data to any fields container, including those to which they have no configured access. Versions 1.13.1 and 1.20.4 contain a patch for this issue. **CVE ID : CVE-2023-28855**	https://github.com/pluginsGLPI/fields/security/advisories/GHSA-52vv-hm4x-8584, https://github.com/pluginsGLPI/fields/commit/784260be7db185bb1e7d66b299997238c4c0205d	A-TEC-FIEL-200423/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: timersys					
Product: wp_popups					
Affected Version(s): * Up to (excluding) 2.1.4.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Timersys WP Popups – WordPress Popup plugin <= 2.1.4.8 versions. **CVE ID : CVE-2023-24003**	N/A	A-TIM-WP_P-200423/617
Vendor: tinytiff_project					
Product: tinytiff					
Affected Version(s): 3.0.0.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Apr-2023	7.8	Buffer Overflow vulnerability found in tinyTIFF v.3.0 allows a local attacker to cause a denial of service via the TinyTiffReader_readNextFrame function in tinytiffreader.c file. **CVE ID : CVE-2023-26733**	https://github.com/jkriege2/TinyTIFF/issues/19	A-TIN-TINY-200423/618
Vendor: torchbox					
Product: wagtail					
Affected Version(s): * Up to (excluding) 4.1.4					
Uncontrolled Resource Consumption	03-Apr-2023	4.9	Wagtail is an open source content management system built on Django. Prior to versions 4.1.4 and 4.2.2, a memory exhaustion	https://github.com/wagtail/wagtail/commit/cfa11bbe00dbe7ce8cd4c0bbfe2a898a690df2bf,	A-TOR-WAGT-200423/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bug exists in Wagtail's handling of uploaded images and documents. For both images and documents, files are loaded into memory during upload for additional processing. A user with access to upload images or documents through the Wagtail admin interface could upload a file so large that it results in a crash of denial of service. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. It can only be exploited by admin users with permission to upload images or documents. Image uploads are restricted to 10MB by default, however this validation only happens on the frontend and on the backend after the vulnerable code. Patched versions have been released as Wagtail 4.1.4 and Wagtail 4.2.2). Site owners who are unable to upgrade to the new versions are	https://github.com/wagtail/wagtail/commit/3c0c64642b9e5b8d28b111263c7f4bddad6c3880, https://github.com/wagtail/wagtail/security/advisories/GHSA-33pv-vcgh-jfg9	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			encouraged to add extra protections outside of Wagtail to limit the size of uploaded files. **CVE ID : CVE-2023-28837**		
Affected Version(s): From (including) 1.5 Up to (excluding) 4.1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Wagtail is an open source content management system built on Django. Starting in version 1.5 and prior to versions 4.1.4 and 4.2.2, a stored cross-site scripting (XSS) vulnerability exists on ModelAdmin views within the Wagtail admin interface. A user with a limited-permission editor account for the Wagtail admin could potentially craft pages and documents that, when viewed by a user with higher privileges, could perform actions with that user's credentials. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin, and only affects sites with ModelAdmin enabled. For page, the vulnerability is in	https://github.com/wagtail/wagtail/security/advisories/GHSA-5286-f2rf-35c2, https://github.com/wagtail/wagtail/commit/5be2b1ed55fd7259dfdf2c82e7701dba407b8b62, https://github.com/wagtail/wagtail/commit/ff806ab173a504395fdfb3139eb0a29444ab4b91	A-TOR-WAGT-200423/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the "Choose a parent page" ModelAdmin view (`ChooseParentView`), available when managing pages via ModelAdmin. For documents, the vulnerability is in the ModelAdmin Inspect view (`InspectView`) when displaying document fields. Patched versions have been released as Wagtail 4.1.4 and Wagtail 4.2.2. Site owners who are unable to upgrade to the new versions can disable or override the corresponding functionality. **CVE ID : CVE-2023-28836**		
Affected Version(s): From (including) 4.2 Up to (excluding) 4.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Apr-2023	5.4	Wagtail is an open source content management system built on Django. Starting in version 1.5 and prior to versions 4.1.4 and 4.2.2, a stored cross-site scripting (XSS) vulnerability exists on ModelAdmin views within the Wagtail admin interface. A user with a limited-permission editor account for the Wagtail admin	https://github.com/wagtail/wagtail/security/advisories/GHSA-5286-f2rf-35c2, https://github.com/wagtail/wagtail/commit/5be2b1ed55fd7259dfdf2c82e7701dba407b8b62, https://github.com/wagtail/wagtail/commit/ff806ab173	A-TOR-WAGT-200423/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could potentially craft pages and documents that, when viewed by a user with higher privileges, could perform actions with that user's credentials. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin, and only affects sites with ModelAdmin enabled. For page, the vulnerability is in the "Choose a parent page" ModelAdmin view (`ChooseParentView`), available when managing pages via ModelAdmin. For documents, the vulnerability is in the ModelAdmin Inspect view (`InspectView`) when displaying document fields. Patched versions have been released as Wagtail 4.1.4 and Wagtail 4.2.2. Site owners who are unable to upgrade to the new versions can disable or override the corresponding functionality. **CVE ID : CVE-2023-28836**	a504395fdfb3139eb0a29444ab4b91	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	03-Apr-2023	4.9	Wagtail is an open source content management system built on Django. Prior to versions 4.1.4 and 4.2.2, a memory exhaustion bug exists in Wagtail's handling of uploaded images and documents. For both images and documents, files are loaded into memory during upload for additional processing. A user with access to upload images or documents through the Wagtail admin interface could upload a file so large that it results in a crash of denial of service. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. It can only be exploited by admin users with permission to upload images or documents. Image uploads are restricted to 10MB by default, however this validation only happens on the frontend and on the backend after the vulnerable code.	https://github.com/wagtail/wagtail/commit/cfa11bbe00dbe7ce8cd4c0bbfe2a898a690df2bf, https://github.com/wagtail/wagtail/commit/3c0c64642b9e5b8d28b111263c7f4bddad6c3880, https://github.com/wagtail/wagtail/security/advisories/GHSA-33pv-vcgh-jfg9	A-TOR-WAGT-200423/622

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patched versions have been released as Wagtail 4.1.4 and Wagtail 4.2.2). Site owners who are unable to upgrade to the new versions are encouraged to add extra protections outside of Wagtail to limit the size of uploaded files. **CVE ID : CVE-2023-28837**		
Vendor: trellix					
Product: agent					
Affected Version(s): * Up to (including) 5.7.8					
Improper Preservation of Permissions	03-Apr-2023	7.8	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 be executed. This allows the user to elevate their permissions. **CVE ID : CVE-2023-0975**	https://kcm.trellix.com/corporate/index?page=content&id=SB10396	A-TRE-AGEN-200423/623
Out-of-bounds Write	03-Apr-2023	6.5	A heap-based overflow vulnerability in Trellix Agent (Windows and Linux) version 5.7.8 and earlier, allows a remote user to alter the page heap in the	https://kcm.trellix.com/corporate/index?page=content&id=SB10396	A-TRE-AGEN-200423/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macmnsvc process memory block resulting in the service becoming unavailable. **CVE ID : CVE-2023-0977**		
Vendor: tribe29					
Product: checkmk					
Affected Version(s): 1.6.0					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/625
Affected Version(s): 1.6.0b10					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			certain configurations. **CVE ID : CVE-2023-1768**		
Affected Version(s): 1.6.0b11					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/627
Affected Version(s): 1.6.0p10					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/628
Affected Version(s): 1.6.0p11					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/629
Affected Version(s): 1.6.0p12					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/630
Affected Version(s): 1.6.0p13					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**		
Affected Version(s): 1.6.0p14					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/632
Affected Version(s): 1.6.0p15					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**		
Affected Version(s): 1.6.0p16					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/634
Affected Version(s): 1.6.0p17					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.6.0p18					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/636
Affected Version(s): 2.0.0					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/637
Affected Version(s): 2.1.0					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**		
Affected Version(s): 2.2.0					
N/A	04-Apr-2023	5.3	Inappropriate error handling in Tribe29 Checkmk <= 2.1.0p25, <= 2.0.0p34, <= 2.2.0b3 (beta), and all versions of Checkmk 1.6.0 causes the symmetric encryption of agent data to fail silently and transmit the data in plaintext in certain configurations. **CVE ID : CVE-2023-1768**	https://checkmk.com/werk/15423	A-TRI-CHEC-200423/639
Vendor: Twitter					
Product: recommendation_algorithm					
Affected Version(s): * Up to (including) 2023-03-31					
N/A	03-Apr-2023	7.5	The Twitter Recommendation Algorithm through ec83d01 allows attackers to cause a denial of service (reduction of reputation score) by	N/A	A-TWI-RECO-200423/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arranging for multiple Twitter accounts to coordinate negative signals regarding a target account, such as unfollowing, muting, blocking, and reporting, as exploited in the wild in March and April 2023. **CVE ID : CVE-2023-29218**		
Vendor: ulearn_project					
Product: ulearn					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	7.2	Ulearn version a5a7ca20de859051ea0470542844980a66dfc05d allows an attacker with administrator permissions to obtain remote code execution on the server through the image upload functionality. This occurs because the application does not validate that the uploaded image is actually an image. **CVE ID : CVE-2023-0670**	N/A	A-ULE-ULEA-200423/641
Vendor: updraftplus					
Product: all-in-one_security					
Affected Version(s): * Up to (excluding) 5.1.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Apr-2023	4.9	The All-In-One Security (AIOS) WordPress plugin before 5.1.5 does not limit what log files to display in it's settings pages, allowing an authorized user (admin+) to view the contents of arbitrary files and list directories anywhere on the server (to which the web server has access). The plugin only displays the last 50 lines of the file. **CVE ID : CVE-2023-0156**	N/A	A-UPD-ALL--200423/642
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	4.8	The All-In-One Security (AIOS) WordPress plugin before 5.1.5 does not escape the content of log files before outputting it to the plugin admin page, allowing an authorized user (admin+) to plant bogus log files containing malicious JavaScript code that will be executed in the context of any administrator visiting this page. **CVE ID : CVE-2023-0157**	N/A	A-UPD-ALL--200423/643
Vendor: uptime_kuma_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: uptime_kuma					
Affected Version(s): * Up to (including) 1.19.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	6.1	Cross Site Scripting vulnerability found in : louislam Uptime Kuma v.1.19.6 and before allows a remote attacker to execute arbitrary commands via the description, title, footer, and incident creation parameter of the status_page.js endpoint. **CVE ID : CVE-2023-26777**	N/A	A-UPT-UPTI-200423/644
Vendor: uvdesk					
Product: community-skeleton					
Affected Version(s): 1.1.1					
Unrestricted Upload of File with Dangerous Type	04-Apr-2023	8.8	Uvdesk version 1.1.1 allows an authenticated remote attacker to execute commands on the server. This is possible because the application does not properly validate profile pictures uploaded by customers. **CVE ID : CVE-2023-0265**	N/A	A-UVD-COMM-200423/645
Improper Neutralization of Input During Web Page Generation	04-Apr-2023	6.1	Uvdesk version 1.1.1 allows an unauthenticated remote attacker to exploit a stored XSS in the application. This is possible	N/A	A-UVD-COMM-200423/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			because the application does not correctly validate the message sent by the clients in the ticket. **CVE ID : CVE-2023-0325**		
Vendor: Veritas					
Product: netbackup_opscenter					
Affected Version(s): 9.1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Veritas NetBackUp OpsCenter Version 9.1.0.1 is vulnerable to Reflected Cross-site scripting (XSS). The Web App fails to adequately sanitize special characters. By leveraging this issue, an attacker is able to cause arbitrary HTML and JavaScript code to be executed in a user's browser. **CVE ID : CVE-2023-26789**	N/A	A-VER-NETB-200423/647
Vendor: vikwp					
Product: vikbooking_hotel_booking_engine_\&_pms					
Affected Version(s): * Up to (excluding) 1.5.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in E4J s.R.L. VikBooking Hotel Booking Engine & PMS plugin <= 1.5.11 versions. **CVE ID : CVE-2023-24396**	N/A	A-VIK-VIKB-200423/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: vitalpbx					
Product: vitalpbx					
Affected Version(s): 3.2.3					
Cross-Site Request Forgery (CSRF)	04-Apr-2023	8.8	VitalPBX version 3.2.3-8 allows an unauthenticated external attacker to obtain the instance administrator's account. This is possible because the application is vulnerable to CSRF. **CVE ID : CVE-2023-0480**	N/A	A-VIT-VITA-200423/649
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	6.1	VitalPBX version 3.2.3-8 allows an unauthenticated external attacker to obtain the instance's administrator account via a malicious link. This is possible because the application is vulnerable to XSS. **CVE ID : CVE-2023-0486**	N/A	A-VIT-VITA-200423/650
Vendor: vm2_project					
Product: vm2					
Affected Version(s): * Up to (excluding) 3.9.15					
Improper Control of Dynamically-Managed Code Resources	06-Apr-2023	9.8	vm2 is a sandbox that can run untrusted code with whitelisted Node's built-in modules. Prior to version 3.9.15, vm2 was not properly handling host objects passed to	https://github.com/patriksimek/vm2/commit/d534e5785f38307b70d3aac1945260a261a94d50, https://github.com/patriksi	A-VM2-VM2-200423/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`Error.prepareStackTrace` in case of unhandled async errors. A threat actor could bypass the sandbox protections to gain remote code execution rights on the host running the sandbox. This vulnerability was patched in the release of version 3.9.15 of vm2. There are no known workarounds. **CVE ID : CVE-2023-29017**	mek/vm2/security/advisories/GHSA-7jxr-cg7f-gpgv	
Vendor: webfactoryltd					
Product: maps_widget_for_google_maps					
Affected Version(s): * Up to (including) 4.24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	The Maps Widget for Google Maps for WordPress is vulnerable to Stored Cross-Site Scripting via widget settings in versions up to, and including, 4.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an	N/A	A-WEB-MAPS-200423/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2023-1913**		
Vendor: wondershare					
Product: anireel					
Affected Version(s): 1.5.4					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd Anireel 1.5.4 allows a remote attacker to execute arbitrary commands via the anireel_setup_full9589.exe file. **CVE ID : CVE-2023-27766**	N/A	A-WON-ANIR-200423/653
Product: creative_centerr					
Affected Version(s): 1.0.8					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd Creative Centerr v.1.0.8 allows a remote attacker to execute arbitrary commands via the wondershareCC_setup_full10819.exe file. **CVE ID : CVE-2023-27771**	N/A	A-WON-CREA-200423/654
Product: democreator					
Affected Version(s): 6.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co., Ltd DemoCreator v.6.0.0 allows a remote attacker to execute arbitrary commands via the democreator_setup_full7743.exe file. **CVE ID : CVE-2023-27762**	N/A	A-WON-DEMO-200423/655
Product: dr.fone					
Affected Version(s): 12.4.9					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd Dr.Fone v.12.4.9 allows a remote attacker to execute arbitrary commands via the drfone_setup_full3360.exe file. **CVE ID : CVE-2023-27767**	N/A	A-WON-DR.F-200423/656
Product: edraw-max					
Affected Version(s): 12.0.4					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd Edraw-max v.12.0.4 allows a remote attacker to execute arbitrary commands via the edraw-max_setup_full5371.exe file. **CVE ID : CVE-2023-27770**	N/A	A-WON-EDRA-200423/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: edrawmind					
Affected Version(s): 10.0.6					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co, Ltd Edrawmind v.10.0.6 allows a remote attacker to executea arbitrary commands via the WindowsCodescs.dll file. **CVE ID : CVE-2023-27759**	N/A	A-WON-EDRA-200423/658
Product: filmora					
Affected Version(s): 12.0.9					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co, Ltd Filmora v.12.0.9 allows a remote attacker to execute arbitrary commands via the filmora_setup_full846.exe. **CVE ID : CVE-2023-27760**	N/A	A-WON-FILM-200423/659
Product: mobiletrans					
Affected Version(s): 4.0.2					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd MobileTrans v.4.0.2 allows a remote attacker to execute arbitrary commands via the mobiletrans_setup_full5793.exe file.	N/A	A-WON-MOBI-200423/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27763		
Product: pdfelement					
Affected Version(s): 9.1.1					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd PDFelement v9.1.1 allows a remote attacker to execute arbitrary commands via the pdfelement-pro_setup_full5239.exe file. **CVE ID : CVE-2023-27768**	N/A	A-WON-PDFE-200423/661
Product: pdf_reader					
Affected Version(s): 1.0.1					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd PDF Reader v.1.0.1 allows a remote attacker to execute arbitrary commands via the pdfreader_setup_full13143.exe file. **CVE ID : CVE-2023-27769**	N/A	A-WON-PDF_-200423/662
Product: recoverit					
Affected Version(s): 10.6.3					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd Recoverit v.10.6.3 allows a remote attacker to execute arbitrary commands via the	N/A	A-WON-RECO-200423/663

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recoverit_setup_full4134.exe file. **CVE ID : CVE-2023-27765**		
Product: repairit					
Affected Version(s): 3.5.4					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co.,Ltd Repairit v.3.5.4 allows a remote attacker to execute arbitrary commands via the repairit_setup_full5913.exe file. **CVE ID : CVE-2023-27764**	N/A	A-WON-REPA-200423/664
Product: uniconverter					
Affected Version(s): 14.0.0					
Untrusted Search Path	04-Apr-2023	7.8	An issue found in Wondershare Technology Co., Ltd UniConverter v.14.0.0 allows a remote attacker to execute arbitrary commands via the uniconverter14_64bit_setup_full14204.exe file. **CVE ID : CVE-2023-27761**	N/A	A-WON-UNIC-200423/665
Vendor: wordpress_amazon_s3_project					
Product: wordpress_amazon_s3					
Affected Version(s): * Up to (excluding) 1.6					
Improper Neutralization of	10-Apr-2023	4.8	The WordPress Amazon S3 Plugin WordPress plugin	N/A	A-WOR-WORD-200423/666

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			before 1.6 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-0423**		
Vendor: wp-buddy					
Product: google_analytics_opt-out					
Affected Version(s): * Up to (excluding) 2.3.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP-Buddy Google Analytics Opt-Out plugin <= 2.3.4 versions. **CVE ID : CVE-2023-25712**	N/A	A-WP--GOOG-200423/667
Vendor: wp-property-hive					
Product: propertyhive					
Affected Version(s): * Up to (excluding) 1.5.47					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in PropertyHive plugin <= 1.5.46 versions. **CVE ID : CVE-2023-29172**	N/A	A-WP--PROP-200423/668
Vendor: Wpbookingsystem					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wp_booking_system					
Affected Version(s): * Up to (including) 2.0.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Veribo, Roland Murg WP Booking System – Booking Calendar plugin <= 2.0.18 versions. **CVE ID : CVE-2023-24402**	N/A	A-WPB-WP_B-200423/669
Vendor: wpdevart					
Product: download_image_and_video_lightbox\,_image_popup					
Affected Version(s): * Up to (excluding) 2.1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Image and Video Lightbox, Image PopUp plugin <= 2.1.5 versions. **CVE ID : CVE-2023-24004**	N/A	A-WPD-DOWN-200423/670
Product: organization_chart					
Affected Version(s): * Up to (excluding) 1.4.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart Organization chart plugin <= 1.4.4 versions. **CVE ID : CVE-2023-24387**	N/A	A-WPD-ORGA-200423/671
Product: responsive_vertical_icon_menu					
Affected Version(s): * Up to (excluding) 1.5.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in wpdevart Responsive Vertical Icon Menu plugin <= 1.5.8 versions. **CVE ID : CVE-2023-23870**	N/A	A-WPD-RESP-200423/672
Product: social_like_box_and_page					
Affected Version(s): * Up to (including) 0.8.39					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Smplug-in Social Like Box and Page by WpDevArt plugin <= 0.8.39 versions. **CVE ID : CVE-2023-23972**	N/A	A-WPD-SOCI-200423/673
Product: youtube_embed\,_playlist_and_popup					
Affected Version(s): * Up to (excluding) 2.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPdevart YouTube Embed, Playlist and Popup by WpDevArt plugin <= 2.6.3 versions. **CVE ID : CVE-2023-24002**	N/A	A-WPD-YOUT-200423/674
Vendor: Wpeasycart					
Product: wp_easycart					
Affected Version(s): * Up to (excluding) 5.4.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Apr-2023	7.2	The Shopping Cart & eCommerce Store WordPress plugin before 5.4.3 does not validate HTTP requests, allowing authenticated users with admin privileges to perform LFI attacks. **CVE ID : CVE-2023-1124**	N/A	A-WPE-WP_E-200423/675
Vendor: wpeverest					
Product: user_registration					
Affected Version(s): * Up to (excluding) 2.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPEverest User Registration plugin <= 2.3.0 versions. **CVE ID : CVE-2023-23987**	N/A	A-WPE-USER-200423/676
Vendor: wpfastestcache					
Product: wp_fastest_cache					
Affected Version(s): * Up to (including) 1.1.2					
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_preload_single_callback function. This makes it possible for	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers to invoke a cache building action via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1918**		
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_preload_single_save_settings_callback function. This makes it possible for unauthenticated attackers to change cache-related settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1919**	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/678
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-	A-WPF-WP_F-200423/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_purgecache_varnish_callback function. This makes it possible for unauthenticated attackers to purge the varnish cache via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1920**	cache/trunk/wpFastestCache.php?contextall=1	
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_start_cdn_integration_ajax_request_callback function. This makes it possible for unauthenticated attackers to change cdn settings via a forged request granted they can trick a site administrator into	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performing an action such as clicking on a link. **CVE ID : CVE-2023-1921**		
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_pause_cdn_integration_ajax_request_callback function. This makes it possible for unauthenticated attackers to change cdn settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1922**	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/681
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_remove_cdn_in	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tegration_ajax_request_callback function. This makes it possible for unauthenticated attackers to change cdn settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1923**		
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_toolbar_save_settings_callback function. This makes it possible for unauthenticated attackers to change cache settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1924**	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the wpfc_clear_cache_of_allsites_callback function. This makes it possible for unauthenticated attackers to clear caches via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1925**	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/684
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the deleteCacheToolbar function. This makes it possible for unauthenticated attackers to perform cache deletion via a forged request granted they can	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1926**		
Cross-Site Request Forgery (CSRF)	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the deleteCssAndJsCacheToolbar function. This makes it possible for unauthenticated attackers to perform cache deletion via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-1927**	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/686
Missing Authorization	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the wpfc_preload_single_callback function in	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 1.1.2. This makes it possible for authenticated attackers with subscriber-level access to initiate cache creation. **CVE ID : CVE-2023-1928**		
Missing Authorization	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data modification due to a missing capability check on the wpfc_purgecache_varnish_callback function in versions up to, and including, 1.1.2. This makes it possible for authenticated attackers with subscriber-level access to purge the varnish cache. **CVE ID : CVE-2023-1929**	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/688
Missing Authorization	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data deletion due to a missing capability check on the wpfc_clear_cache_of_allsites_callback function in versions up to, and including,	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.1.2. This makes it possible for authenticated attackers with subscriber-level access to delete caches. **CVE ID : CVE-2023-1930**		
Missing Authorization	06-Apr-2023	4.3	The WP Fastest Cache plugin for WordPress is vulnerable to unauthorized data loss due to a missing capability check on the deleteCssAndJsCacheToolbar function in versions up to, and including, 1.1.2. This makes it possible for authenticated attackers with subscriber-level access to perform cache deletion. **CVE ID : CVE-2023-1931**	https://plugins.trac.wordpress.org/changeset/2893158/wp-fastest-cache/trunk/wpFastestCache.php?contextall=1	A-WPF-WP_F-200423/690
Vendor: wpforthewin					
Product: bbpress_voting					
Affected Version(s): * Up to (excluding) 2.1.11.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP For The Win bbPress Voting plugin <= 2.1.11.0 versions. **CVE ID : CVE-2023-24403**	N/A	A-WPF-BBPR-200423/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpfrom_email_project					
Product: wpfrom_email					
Affected Version(s): * Up to (excluding) 1.8.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Apr-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPGear.Pro WPFrom Email plugin <= 1.8.8 versions. **CVE ID : CVE-2023-23982**	N/A	A-WPF-WPFR-200423/692
Vendor: wpglobus					
Product: wpglobus_translate_options					
Affected Version(s): * Up to (excluding) 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPGlobus WPGlobus Translate Options plugin <= 2.1.0 versions. **CVE ID : CVE-2023-25711**	N/A	A-WPG-WPGL-200423/693
Vendor: xml2js_project					
Product: xml2js					
Affected Version(s): 0.4.23					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	05-Apr-2023	5.3	xml2js version 0.4.23 allows an external attacker to edit or add new properties to an object. This is possible because the application does not properly validate incoming JSON keys, thus allowing the	N/A	A-XML-XML2-200423/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__proto__ property to be edited. **CVE ID : CVE-2023-0842**		
Vendor: xuxueli					
Product: xxl-job					
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Apr-2023	6.1	This affects all versions of the package com.xuxueli:xxl-job. HTML uploaded payload executed successfully through /xxl-job-admin/user/add and /xxl-job-admin/user/update. **CVE ID : CVE-2023-26120**	N/A	A-XUX-XXL--200423/695
Vendor: Yiiframework					
Product: yii					
Affected Version(s): From (including) 2.0.0 Up to (including) 2.0.47					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Apr-2023	9.8	** DISPUTED ** SQL injection vulnerability found in Yii Framework Yii 2 Framework before v.2.0.47 allows the a remote attacker to execute arbitrary code via the runAction function. NOTE: the software maintainer's position is that the vulnerability is in third-party code, not in the framework.	N/A	A-YII-YII-200423/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26750		
Vendor: zeno_font_resizer_project					
Product: zeno_font_resizer					
Affected Version(s): * Up to (excluding) 1.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Apr-2023	4.8	Auth. (admin+) Stored Cross-site Scripting (XSS) vulnerability in Marcel Pol Zeno Font Resizer plugin <= 1.7.9 versions. **CVE ID : CVE-2023-25442**	N/A	A-ZEN-ZENO-200423/697
Vendor: Zohocorp					
Product: manageengine_adselfservice_plus					
Affected Version(s): 5.1					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/698
Affected Version(s): 4.5					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/699
Affected Version(s): 5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/700
Affected Version(s): 5.0.6					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/701
Affected Version(s): 5.2					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/702
Affected Version(s): 5.3					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API.	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28342		
Affected Version(s): 5.4					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/704
Affected Version(s): 5.5					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/705
Affected Version(s): 5.6					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/706
Affected Version(s): 5.7					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a	https://www.manageengine.com/products/self-service-	A-ZOH-MANA-200423/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	password/advisory/CVE-2023-28342.html	
Affected Version(s): 5.8					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/708
Affected Version(s): 6.0					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/709
Affected Version(s): 6.1					
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/710
Affected Version(s): 6.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Apr-2023	7.5	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API. **CVE ID : CVE-2023-28342**	https://www.manageengine.com/products/self-service-password/advisory/CVE-2023-28342.html	A-ZOH-MANA-200423/711
Product: manageengine_applications_manager					
Affected Version(s): * Up to (excluding) 16.3					
Improper Restriction of XML External Entity Reference	11-Apr-2023	6.5	Zoho ManageEngine Applications Manager through 16320 allows the admin user to conduct an XXE attack. **CVE ID : CVE-2023-28340**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-28340.html	A-ZOH-MANA-200423/712
Affected Version(s): 15.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	6.1	Stored Cross site scripting (XSS) vulnerability in Zoho ManageEngine Applications Manager through 16340 allows an unauthenticated user to inject malicious javascript on the incorrect login details page. **CVE ID : CVE-2023-28341**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-28341.html	A-ZOH-MANA-200423/713
Affected Version(s): 16.3					
Improper Restriction of XML	11-Apr-2023	6.5	Zoho ManageEngine Applications Manager through	https://www.manageengine.com/product	A-ZOH-MANA-200423/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			16320 allows the admin user to conduct an XXE attack. **CVE ID : CVE-2023-28340**	s/applications_manager/security-updates/security-updates-cve-2023-28340.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	6.1	Stored Cross site scripting (XSS) vulnerability in Zoho ManageEngine Applications Manager through 16340 allows an unauthenticated user to inject malicious javascript on the incorrect login details page. **CVE ID : CVE-2023-28341**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-28341.html	A-ZOH-MANA-200423/715
Affected Version(s): From (including) 16.0 Up to (excluding) 16.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	6.1	Stored Cross site scripting (XSS) vulnerability in Zoho ManageEngine Applications Manager through 16340 allows an unauthenticated user to inject malicious javascript on the incorrect login details page. **CVE ID : CVE-2023-28341**	https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2023-28341.html	A-ZOH-MANA-200423/716
Hardware					
Vendor: AMD					
Product: athlon_gold_3150u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-ATHL-200423/717
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-ATHL-200423/718
Product: athlon_silver_3050u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-ATHL-200423/719
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSm	https://www.amd.com/en/resources/pro	H-AMD-ATHL-200423/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			m may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	duct-security/bulletin/amd-sb-1027.html	
Product: ryzen_3_2200u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/721
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/722
Product: ryzen_3_2300u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a	https://www.amd.com/en/resources/product-	H-AMD-RYZE-200423/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/724
Product: ryzen_3_3200u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/725
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/726

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**		
Product: ryzen_3_3250u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/727
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/728
Product: ryzen_3_3300u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an escalation of privileges. **CVE ID : CVE-2023-20558**		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/730
Product: ryzen_3_3300x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/731
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_3_3350u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/733
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/734
Product: ryzen_3_3450u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/736
Product: ryzen_3_3500c					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/737
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/738
Product: ryzen_3_3500u					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/739
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/740
Product: ryzen_3_3550h					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/741
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	H-AMD-RYZE-200423/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_3_3580u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/743
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/744
Product: ryzen_3_3700c					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	H-AMD-RYZE-200423/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/746
Product: ryzen_3_3700u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/747
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_3_3750h					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/749
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/750
Product: ryzen_3_3780u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/752
Product: ryzen_3_4300g					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/753
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_3_4300ge					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/755
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/756
Product: ryzen_3_5125c					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/758
Product: ryzen_3_5300g					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/759
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/760
Product: ryzen_3_5300ge					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/761
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/762
Product: ryzen_3_5400u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/763
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	H-AMD-RYZE-200423/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_3_5425c					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/765
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/766
Product: ryzen_3_5425u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	H-AMD-RYZE-200423/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/768
Product: ryzen_5_2500u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/769
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_5_2600					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/771
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/772
Product: ryzen_5_2600h					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/774
Product: ryzen_5_2600x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/775
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_5_2700					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/777
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/778
Product: ryzen_5_2700x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/780
Product: ryzen_5_3500					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/781
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/782
Product: ryzen_5_3500x					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/783
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/784
Product: ryzen_5_3600					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/785
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	H-AMD-RYZE-200423/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_5_3600x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/787
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/788
Product: ryzen_5_3600xt					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	H-AMD-RYZE-200423/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/790
Product: ryzen_5_4600g					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/791
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/792

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_5_4600ge					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/793
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/794
Product: ryzen_5_5560u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/796
Product: ryzen_5_5600g					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/797
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/798

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_5_5600ge					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/799
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/800
Product: ryzen_5_5600h					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/802
Product: ryzen_5_5600hs					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/803
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/804
Product: ryzen_5_5600u					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/805
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/806
Product: ryzen_5_5625c					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/807
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	H-AMD-RYZE-200423/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_5_5625u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/809
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/810
Product: ryzen_7_2700					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	H-AMD-RYZE-200423/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/812
Product: ryzen_7_2700u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/813
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_7_2700x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/815
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/816
Product: ryzen_7_2800h					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/818
Product: ryzen_7_3700x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/819
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_7_3800x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/821
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/822
Product: ryzen_7_3800xt					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/824
Product: ryzen_7_4700g					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/825
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/826
Product: ryzen_7_4700ge					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/827
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/828
Product: ryzen_7_5700g					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/829
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	H-AMD-RYZE-200423/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_7_5700ge					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/831
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/832
Product: ryzen_7_5800h					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	H-AMD-RYZE-200423/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/834
Product: ryzen_7_5800hs					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/835
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_7_5800u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/837
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/838
Product: ryzen_7_5825c					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/840
Product: ryzen_7_5825u					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/841
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_9_3900					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/843
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/844
Product: ryzen_9_3900x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/846
Product: ryzen_9_3900xt					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/847
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/848
Product: ryzen_9_3950x					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/849
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/850
Product: ryzen_9_5900hs					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/851
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	H-AMD-RYZE-200423/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_9_5900hx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/853
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/854
Product: ryzen_9_5980hs					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	H-AMD-RYZE-200423/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/856
Product: ryzen_9_5980hx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/857
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_9_pro_3900					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/859
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/860
Product: ryzen_threadripper_2920x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/862
Product: ryzen_threadripper_2950x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/863
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_threadripper_2970wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/865
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/866
Product: ryzen_threadripper_2990wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/868
Product: ryzen_threadripper_3960x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/869
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/870
Product: ryzen_threadripper_3970x					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/871
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/872
Product: ryzen_threadripper_3990x					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/873
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	H-AMD-RYZE-200423/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_threadripper_pro_3795wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/875
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/876
Product: ryzen_threadripper_pro_3945wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	H-AMD-RYZE-200423/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/878
Product: ryzen_threadripper_pro_3955wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/879
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_threadripper_pro_3975wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/881
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/882
Product: ryzen_threadripper_pro_3995wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	H-AMD-RYZE-200423/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/884
Product: ryzen_threadripper_pro_5945wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/885
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_threadripper_pro_5955wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/887
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/888
Product: ryzen_threadripper_pro_5965wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/890
Product: ryzen_threadripper_pro_5975wx					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/891
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/892
Product: ryzen_threadripper_pro_5995wx					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/893
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	H-AMD-RYZE-200423/894
Vendor: Aten					
Product: pe8108					
Affected Version(s): -					
Insufficiently Protected Credentials	11-Apr-2023	7.5	Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. The device allows unauthenticated access to Telnet and SNMP credentials. **CVE ID : CVE-2023-25413**	https://www.pentagrid.ch/en/blog/multiple-vulnerabilities-in-aten-PE8108-power-distribution-unit/	H-ATE-PE81-200423/895
Insufficiently	11-Apr-2023	7.2	Aten PE8108 2.4.232 is vulnerable to Incorrect Access	https://www.pentagrid.ch/en/blog/multi	H-ATE-PE81-200423/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Control. Restricted users have read access to administrator credentials. **CVE ID : CVE-2023-25407**	ple-vulnerabilities-in-aten-PE8108-power-distribution-unit/	
N/A	11-Apr-2023	5.3	Aten PE8108 2.4.232 is vulnerable to denial of service (DOS). **CVE ID : CVE-2023-25414**	N/A	H-ATE-PE81-200423/897
Incorrect Authorization	11-Apr-2023	5.3	Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. The device allows unauthenticated access to Event Notification configuration. **CVE ID : CVE-2023-25415**	N/A	H-ATE-PE81-200423/898
Cross-Site Request Forgery (CSRF)	11-Apr-2023	4.3	Aten PE8108 2.4.232 is vulnerable to Cross Site Request Forgery (CSRF). **CVE ID : CVE-2023-25411**	https://www.pentagrid.ch/en/blog/multiple-vulnerabilities-in-aten-PE8108-power-distribution-unit/	H-ATE-PE81-200423/899
Vendor: Buffalo					
Product: bs-gs2008					
Affected Version(s): -					
Improper Neutralization of Input	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network	https://www.buffalo.jp/news/detail/202	H-BUF-BS-G-200423/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**	30310-01.html	
Product: bs-gs2008p					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to	https://www.buffalo.jp/news/detail/20230310-01.html	H-BUF-BS-G-200423/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2016					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products	https://www.buffalo.jp/news/detail/20230310-01.html	H-BUF-BS-G-200423/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2016p					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware	https://www.buffalo.jp/news/detail/20230310-01.html	H-BUF-BS-G-200423/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2024					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware	https://www.buffalo.jp/news/detail/20230310-01.html	H-BUF-BS-G-200423/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2024p					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P	https://www.buffalo.jp/news/detail/20230310-01.html	H-BUF-BS-G-200423/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2048					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P	https://www.buffalo.jp/news/detail/20230310-01.html	H-BUF-BS-G-200423/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Vendor: Cisco					
Product: asr_5000					
Affected Version(s): -					
N/A	05-Apr-2023	7.5	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 vulnerability by sending a malformed Encapsulating Security Payload (ESP) packet over an IPsec connection. A successful exploit could allow the attacker to stop ICMP traffic over an IPsec connection and cause a denial of service (DoS). **CVE ID : CVE-2023-20051**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pdng-dos-KmzwEy2Q	H-CIS-ASR_-200423/907
Product: asr_5500					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	05-Apr-2023	7.5	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 vulnerability by sending a malformed Encapsulating Security Payload (ESP) packet over an IPsec connection. A successful exploit could allow the attacker to stop ICMP traffic over an IPsec connection and cause a denial of service (DoS). **CVE ID : CVE-2023-20051**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pdng-dos-KmzwEy2Q	H-CIS-ASR_-200423/908
Product: asr_5700					
Affected Version(s): -					
N/A	05-Apr-2023	7.5	A vulnerability in the Vector Packet Processor (VPP) of Cisco Packet Data Network Gateway (PGW) could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-ASR_-200423/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 vulnerability by sending a malformed Encapsulating Security Payload (ESP) packet over an IPsec connection. A successful exploit could allow the attacker to stop ICMP traffic over an IPsec connection and cause a denial of service (DoS). **CVE ID : CVE-2023-20051**	o-sa-cisco-pdng-dos-KmzwEy2Q	
Product: rv016					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	H-CIS-RV01-200423/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-RV01-200423/912

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20138**	o-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/914

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV01-200423/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20145**	stored-xss-vqz7gC8W	
Improper Neutralizat	05-Apr-2023	6.1	Multiple vulnerabilities in the	https://sec.cloudapps.cisco.c	H-CIS-RV01-200423/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that address these vulnerabilities. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20147**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV01-200423/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20151**		
Product: rv042					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command	05-Apr-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	H-CIS-RV04-200423/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**	rv01x_rv32x_rce-nzAGWWDD	
Improper Neutralization of Input During	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-RV04-200423/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates that address these vulnerabilities.	Advisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20137		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-RV04-200423/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20144**	o-sa-rv-stored-xss-vqz7gC8W	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/940

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV04-200423/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20151**	stored-xss-vqz7gC8W	
Product: rv042g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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 credentials on the affected device. Cisco has not released software updates that address this vulnerability.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	H-CIS-RV04-200423/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20124		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-RV04-200423/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20143**	o-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV04-200423/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV04-200423/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20150**	stored-xss-vqz7gC8W	
Improper Neutralizat	05-Apr-2023	6.1	Multiple vulnerabilities in the	https://sec.cloudapps.cisco.c	H-CIS-RV04-200423/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that address these vulnerabilities. **CVE ID : CVE-2023-20151**		
Product: rv082					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	H-CIS-RV08-200423/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/960

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-RV08-200423/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities.	Advisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20142		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/968

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-RV08-200423/971

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20149**	o-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV08-200423/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20151**		
Product: rv320					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL	H-CIS-RV32-200423/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. **CVE ID : CVE-2023-20117**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	H-CIS-RV32-200423/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL	H-CIS-RV32-200423/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. **CVE ID : CVE-2023-20128**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-RV32-200423/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities.	/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20139		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/981

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-RV32-200423/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20146**	o-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20147**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20151**		
Product: rv325					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL	H-CIS-RV32-200423/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. **CVE ID : CVE-2023-20117**		
Improper Neutralization of Special Elements used in a	05-Apr-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV016, RV042,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-RV32-200423/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**	o-sa-sb-rv01x_rv32x_rce-nzAGWWDD	
Improper Neutralization of Special	05-Apr-2023	7.2	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	H-CIS-RV32-200423/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')		🟧	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 credentials on the affected device. Cisco has not released software updates to address these vulnerabilities.	/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20128		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/999

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-RV32-200423/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20143**	o-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	H-CIS-RV32-200423/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	H-CIS-RV32-200423/1008

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20150**	stored-xss-vqz7gC8W	
Improper Neutralizat	05-Apr-2023	6.1	Multiple vulnerabilities in the	https://sec.cloudapps.cisco.c	H-CIS-RV32-200423/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that address these vulnerabilities. **CVE ID : CVE-2023-20151**		
Product: rv340					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	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 successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V	H-CIS-RV34-200423/1010
Product: rv340w					
Affected Version(s): -					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	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 successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V	H-CIS-RV34-200423/1011
Product: rv345					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	A vulnerability in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-	H-CIS-RV34-200423/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**	afu-EXxwA65V	
Product: rv345p					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V	H-CIS-RV34-200423/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of file uploads. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**		
Product: stealthwatch_management_console_2200					
Affected Version(s): -					
Deserialization of Untrusted Data	05-Apr-2023	8.8	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 to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealthsmc-rce-sfNBPjcS	H-CIS-STEA-200423/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying operating system as the administrator user. **CVE ID : CVE-2023-20102**		
Vendor: Dlink					
Product: dir-878					
Affected Version(s): -					
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_475FB0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-24798**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--200423/1015
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_48AF78 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-24799**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--200423/1016
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR878 DIR_878_FW120B05 was discovered to	https://www.dlink.com/en/	H-DLI-DIR--200423/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow in the sub_495220 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-24800**	security-bulletin/	
Out-of-bounds Write	09-Apr-2023	9.8	D-Link DIR878 1.30B08 was discovered to contain a stack overflow in the sub_48d630 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27720**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--200423/1018
Product: dir-882_a1					
Affected Version(s): -					
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR882 DIR882A1_FW110B02 was discovered to contain a stack overflow in the sub_48AC20 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload.	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--200423/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24797		
Product: dir878					
Affected Version(s): -					
Out-of-bounds Write	09-Apr-2023	9.8	D-Link DIR878 1.30B08 was discovered to contain a stack overflow in the sub_498308 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27718**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR8-200423/1020
Product: go-rt-ac750					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Apr-2023	9.8	D-Link Go-RT-AC750 revA_v101b03 was discovered to contain a command injection vulnerability via the service parameter at soapcgi.main. **CVE ID : CVE-2023-26822**	N/A	H-DLI-GO-R-200423/1021
Vendor: getnexx					
Product: nxal-100					
Affected Version(s): -					
Authorization Bypass Through User-	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid	N/A	H-GET-NXAL-200423/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			NexxHome deviceId could retrieve device history, set device settings, and retrieve device information. **CVE ID : CVE-2023-1750**		
Authorization Bypass Through User-Controlled Key	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute. **CVE ID : CVE-2023-1749**	N/A	H-GET-NXAL-200423/1023
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	H-GET-NXAL-200423/1024
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow	N/A	H-GET-NXAL-200423/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any user to register an already registered alarm or associated device with only the device’s MAC address. **CVE ID : CVE-2023-1752**		
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**	N/A	H-GET-NXAL-200423/1026
Product: nxg-100b					
Affected Version(s): -					
Authorization Bypass Through User-Controlled Key	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device	N/A	H-GET-NXG--200423/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings, and retrieve device information. **CVE ID : CVE-2023-1750**		
Authorization Bypass Through User-Controlled Key	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute. **CVE ID : CVE-2023-1749**	N/A	H-GET-NXG--200423/1028
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	H-GET-NXG--200423/1029
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated	N/A	H-GET-NXG--200423/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device with only the device's MAC address. **CVE ID : CVE-2023-1752**		
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**	N/A	H-GET-NXG--200423/1031
Product: nxg-200					
Affected Version(s): -					
Authorization Bypass Through User-Controlled Key	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device settings, and retrieve device information.	N/A	H-GET-NXG--200423/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1750		
Authorization Bypass Through User-Controlled Key	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute. **CVE ID : CVE-2023-1749**	N/A	H-GET-NXG--200423/1033
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	H-GET-NXG--200423/1034
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated device with only the	N/A	H-GET-NXG--200423/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device's MAC address. **CVE ID : CVE-2023-1752**		
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**	N/A	H-GET-NXG--200423/1036
Product: nxpg-100w					
Affected Version(s): -					
Authorization Bypass Through User-Controlled Key	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device settings, and retrieve device information. **CVE ID : CVE-2023-1750**	N/A	H-GET-NXPG-200423/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute. **CVE ID : CVE-2023-1749**	N/A	H-GET-NXPG-200423/1038
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	H-GET-NXPG-200423/1039
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated device with only the device's MAC address.	N/A	H-GET-NXPG-200423/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1752		
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**	N/A	H-GET-NXPG-200423/1041
Vendor: greenpacket					
Product: ot-235					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2023	9.8	GreenPacket OH736's WR-1200 Indoor Unit, OT-235 with firmware versions M-IDU-1.6.0.3_V1.1 and MH-46360-2.0.3-R5-GP respectively are vulnerable to remote command injection. Commands are executed using pre-login execution and executed with root	N/A	H-GRE-OT-2-200423/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges allowing complete takeover. **CVE ID : CVE-2023-26866**		
Product: wr-1200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2023	9.8	GreenPacket OH736's WR-1200 Indoor Unit, OT-235 with firmware versions M-IDU-1.6.0.3_V1.1 and MH-46360-2.0.3-R5-GP respectively are vulnerable to remote command injection. Commands are executed using pre-login execution and executed with root privileges allowing complete takeover. **CVE ID : CVE-2023-26866**	N/A	H-GRE-WR-1-200423/1043
Vendor: mediatek					
Product: mt2715					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT27-200423/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT27-200423/1045
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT27-200423/1046
Product: mt5221					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1047
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1048
Integer Overflow or Wraparound	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. **CVE ID : CVE-2023-20662**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1050
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1052
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1053
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-	H-MED-MT52-200423/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588569. **CVE ID : CVE-2023-20675**	security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1055
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT52-200423/1057
Product: mt6580					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1059
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1061
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1062
Use After Free	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1064
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20682		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT65-200423/1066
Product: mt6731					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1068
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1069
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1070

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6735					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1071
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1073
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1075
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1076
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1078
Product: mt6737					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1080
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1082
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1083
Use After Free	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1084

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1085
Product: mt6739					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1087
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1089
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1090
Use After Free	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1091

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1092
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1094
Product: mt6753					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1096
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1097
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1099
Use After Free	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1101
Product: mt6757					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20652		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1103
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1104
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07441821. **CVE ID : CVE-2023-20688**	bulletin/April-2023	
Product: mt6757c					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1106
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1108
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6757cd					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1110
Out-of-bounds Write	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20653		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1112
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1113
Product: mt6757ch					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1114
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1115
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1116

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1117
Product: mt6761					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1119
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1121
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1122
Use After Free	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1124
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1126
Product: mt6762					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20652		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1128
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1129
Out-of-bounds Read	06-Apr-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20665**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1131
Product: mt6763					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1133
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1135
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1136
Product: mt6765					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1137
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1138
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1140
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1142
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1143
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1145
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1147
Product: mt6768					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20655		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1149
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1150
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1151

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07589148. **CVE ID : CVE-2023-20654**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1152
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1154
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1155
Integer Overflow	06-Apr-2023	6.7	In wlan, there is a possible out of	https://corp.mediatek.com	H-MED-MT67-200423/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	/product-security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1157
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6769					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1159
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1161
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1163
Product: mt6771					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1164
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1166
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1167

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1168
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1170
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1171
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1173
Product: mt6779					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1175
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1177
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1178
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1180
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20670		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1182
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1183
Out-of-bounds Read	06-Apr-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1185
Product: mt6781					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1187
Out-of-bounds Write	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20653		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1189
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1190
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1192
Use After Free	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1194
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1196
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1197
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588569. **CVE ID : CVE-2023-20675**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1199
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1201
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1202
Product: mt6785					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1203
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1204
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1206
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1208
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1209
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	bulletin/April-2023	
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1211
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1213
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6789					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1215
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1216
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1218
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1220
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1222
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1223
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1225
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20685		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1227
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1228
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT67-200423/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588569. **CVE ID : CVE-2023-20675**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1230
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1232
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT67-200423/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20688		
Product: mt6833					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1234
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1236
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1237
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1239
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1240

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1241
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1242
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1244
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1246
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1248
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1249
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1251
Product: mt6853					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1253
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1254

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1255
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1256
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1258
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20670		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1260
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1261
Out-of-bounds Read	06-Apr-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1263
Product: mt6853t					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1265
Out-of-bounds Write	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20653		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1267
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1268
Use After Free	06-Apr-2023	6.7	In gz, there is a possible double free due to a use after free. This could lead	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1270
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1272
Product: mt6855					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20655		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1274
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1275
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07589148. **CVE ID : CVE-2023-20654**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1277
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1279
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1281
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1282
Concurrent Execution using Shared Resource with Improper	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1284
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1285

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1286
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1288
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1289
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1291
Product: mt6873					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1293
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1295
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1296
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1297

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1298
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20670		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1300
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1301
Out-of-bounds Read	06-Apr-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1303
Product: mt6875					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1305
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1307
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1308
Product: mt6877					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1309
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1310
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1312
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1314
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1315
Use After Free	06-Apr-2023	6.7	In gz, there is a possible double free	https://corp.mediatek.com	H-MED-MT68-200423/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20664**	/product-security-bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1317
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1319
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1321
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1322
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1324
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1326
Product: mt6879					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1328
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1329
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1330

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1331
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1333
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1334
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-200423/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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. **CVE ID : CVE-2023-20662**	security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1336
Use After Free	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1337

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1338
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1339
Concurrent Execution	06-Apr-2023	6.4	In vdec, there is a possible use after	https://corp.mediatek.com	H-MED-MT68-200423/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	/product-security-bulletin/April-2023	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1341
Concurrent Execution using Shared Resource with Improper Synchronization	06-Apr-2023	6.4	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 needed for	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1342

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826. **CVE ID : CVE-2023-20686**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772. **CVE ID : CVE-2023-20687**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1343
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1345
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1346
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588569. **CVE ID : CVE-2023-20675**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1348
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1350
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1351
Product: mt6883					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1352
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1353
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1355
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1357
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1358
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1360
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6885					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1362
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1363

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20652		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1364
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1365
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1366

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20656**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1367
Use After Free	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1369
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1370
Integer Overflow	06-Apr-2023	6.7	In wlan, there is a possible out of	https://corp.mediatek.com	H-MED-MT68-200423/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	/product-security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1372
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6886					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1374
Product: mt6889					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1376
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1378
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1379
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1381
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20670		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1383
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1384
Product: mt6891					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1385
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1386
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1388
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6893					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1390
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1392
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1393
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1395
Use After Free	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20664		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1397
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1398
Out-of-bounds Read	06-Apr-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20665**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1400
Product: mt6895					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1402
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1404
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1405
Out-of-bounds Write	06-Apr-2023	6.7	In isp, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT68-200423/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**	security-bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1407
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1409
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1411
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1412
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1414
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1416
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1417
Concurrent Execution using Shared	06-Apr-2023	6.4	In display drm, there is a possible double free due to a race condition. This could	https://corp.mediatek.com/product-security-	H-MED-MT68-200423/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826. **CVE ID : CVE-2023-20686**	bulletin/April-2023	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772. **CVE ID : CVE-2023-20687**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1419
Integer Overflow or Wraparound	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1421
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1423
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1424
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1426
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT68-200423/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6983					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1428
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1430
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1431
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1432

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1433
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07537393;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1435
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1436
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT69-200423/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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. **CVE ID : CVE-2023-20662**	security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1438
Use After Free	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1440
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1441
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of	https://corp.mediatek.com	H-MED-MT69-200423/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	/product-security-bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1443
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1445
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826. **CVE ID : CVE-2023-20686**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1447
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772. **CVE ID : CVE-2023-20687**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1448
Integer Overflow or Wraparound	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1450
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20674		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1452
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1453
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT69-200423/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20677**	bulletin/April -2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April -2023	H-MED-MT69-200423/1455
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April -2023	H-MED-MT69-200423/1456

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt6985					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT69-200423/1457
Product: mt7663					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1459
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1461
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1462
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1464
Product: mt7668					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1466
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1468
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1469
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT76-200423/1471
Product: mt7902					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1473
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1475
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1476
Integer Overflow or Wraparound	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1478
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20675		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1480
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1481
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT79-200423/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588453. **CVE ID : CVE-2023-20679**	bulletin/April-2023	
Product: mt7921					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1483
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1485
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20663		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1487
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1488
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1490
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07588569; Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1492
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1493
Product: mt7933					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT79-200423/1494
Product: mt8167					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1495
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT81-200423/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1497
Product: mt8167s					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1499
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20661		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1501
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1502
Integer Overflow or Wraparound	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1504
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1506
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1508
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1509
Product: mt8168					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format	https://corp.mediatek.com/product-security-	H-MED-MT81-200423/1510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1511
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1513
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1514
Use After Free	06-Apr-2023	6.7	In gz, there is a possible double free due to a use after	https://corp.mediatek.com/product-	H-MED-MT81-200423/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20664**	security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1516
Integer Overflow or Wraparound	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1518
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1520
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1521
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1523
Product: mt8169					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1525
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1527
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1528
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1530
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt8173					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1532
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8175					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1534
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1535
Integer Overflow or Wraparound	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to	https://corp.mediatek.com/product-security-	H-MED-MT81-200423/1536

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**	bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1537
Integer Overflow or Wraparound	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07560741. **CVE ID : CVE-2023-20663**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1539
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1540
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT81-200423/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588552. **CVE ID : CVE-2023-20674**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1542
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1544
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20679		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1546
Product: mt8183					
Affected Version(s): -					
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1547
Product: mt8185					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1548
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1549
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1551
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1553
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1554
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT81-200423/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588552. **CVE ID : CVE-2023-20674**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1556
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1557

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1558
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20679		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1560
Product: mt8188					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1562
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1563
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1564

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1565
Product: mt8192					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1567
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1569
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1570
Product: mt8195					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format	https://corp.mediatek.com/product-security-	H-MED-MT81-200423/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1572
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07310651; Issue ID: ALPS07292173. **CVE ID : CVE-2023-20666**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1574
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT81-200423/1575

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8321					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1576
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1577
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT83-200423/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1579
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1581
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1582
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT83-200423/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1584
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt8362a					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1586
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1588
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1589
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT83-200423/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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 ID : CVE-2023-20663**	bulletin/April-2023	
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1591
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1593
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1594
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-	H-MED-MT83-200423/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588569. **CVE ID : CVE-2023-20675**	security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1596
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1597

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1598
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20688		
Product: mt8365					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1600
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1601
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT83-200423/1602

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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. **CVE ID : CVE-2023-20661**	security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1603
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07560741; Issue ID: ALPS07560741. **CVE ID : CVE-2023-20663**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1605
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1606
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT83-200423/1607

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	security-bulletin/April-2023	
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1608
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1610
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1612
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1613
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588569. **CVE ID : CVE-2023-20675**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1615
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1617
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1618
Product: mt8385					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1619
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1620
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1621

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1622
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1624
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1625
Integer Overflow	06-Apr-2023	6.7	In wlan, there is a possible out of	https://corp.mediatek.com	H-MED-MT83-200423/1626

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			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. **CVE ID : CVE-2023-20661**	/product-security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1627
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. **CVE ID : CVE-2023-20663**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1629
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1630
Integer Overflow	06-Apr-2023	6.7	In wlan, there is a possible out of	https://corp.mediatek.com	H-MED-MT83-200423/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	/product-security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1632
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1634
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20676		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1636
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1637
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT83-200423/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07441821. **CVE ID : CVE-2023-20688**	bulletin/April-2023	
Product: mt8390					
Affected Version(s): -					
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT83-200423/1639
Product: mt8395					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could	https://corp.mediatek.com/product-security-	H-MED-MT83-200423/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	bulletin/April -2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp. mediatek.com /product-security-bulletin/April -2023	H-MED-MT83-200423/1641
Product: mt8518					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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.	https://corp. mediatek.com /product-security-bulletin/April -2023	H-MED-MT85-200423/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1643
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1645
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1646
Integer Overflow or Wraparound	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1647

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1648
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20675		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1650
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1651
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT85-200423/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588453. **CVE ID : CVE-2023-20679**	bulletin/April-2023	
Product: mt8532					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1653
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1655
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20663		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1657
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1658
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1660
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07588569; Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1662
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT85-200423/1663
Product: mt8666					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1664
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1665
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1667
Use After Free	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1669
Product: mt8667					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1671
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1672
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1673

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Product: mt8673					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1674
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1676
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1678
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1679
Concurrent Execution using Shared Resource with Improper Synchronization	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1680

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1681
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20688		
Product: mt8675					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1683
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1685
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1686
Out-of-bounds Write	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1688
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1690
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1691
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-	H-MED-MT86-200423/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07588569. **CVE ID : CVE-2023-20675**	security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1693
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1695
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20688		
Product: mt8695					
Affected Version(s): -					
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1697
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1699
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1700
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1702
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Product: mt8696					
Affected Version(s): -					
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1704
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1706
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1707
Out-of-bounds Write	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1709
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT86-200423/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20688		
Product: mt8765					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1711
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1713
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1714
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1715

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1716
Use After Free	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20664		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1718
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1719
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07441821. **CVE ID : CVE-2023-20688**	bulletin/April-2023	
Product: mt8766					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1721
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1723
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1725
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1726
Out-of-bounds Write	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT87-200423/1727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20659**	security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1728
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1729

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. **CVE ID : CVE-2023-20662**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1730
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1731
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT87-200423/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1733
Integer Overflow or Wraparound	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1735
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1737
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1738
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588436. **CVE ID : CVE-2023-20677**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1740
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt8768					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1742
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1743

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1744
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1745
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1747
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1749
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1750
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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 ID : CVE-2023-20663**	bulletin/April-2023	
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1752
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1754
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1755
Out-of-bounds Read	06-Apr-2023	4.4	In ril, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1756

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20665**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1757
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588569. **CVE ID : CVE-2023-20675**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1759
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20677		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1761
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1762
Product: mt8771					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1763
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1764
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1765

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1766
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1768
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1769
Integer Overflow	06-Apr-2023	6.7	In wlan, there is a possible out of	https://corp.mediatek.com	H-MED-MT87-200423/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			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. **CVE ID : CVE-2023-20661**	/product-security-bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1771
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. **CVE ID : CVE-2023-20663**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1773
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1774
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of	https://corp.mediatek.com	H-MED-MT87-200423/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	/product-security-bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1776
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1778
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20665		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1780
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1781
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07628518. **CVE ID : CVE-2023-20676**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1783
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1785
Product: mt8781					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1786

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20655		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1787
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1788
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07589148. **CVE ID : CVE-2023-20654**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1790
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1792
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1794
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1795
Use After Free	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1797
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20670		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1799
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1800
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	bulletin/April-2023	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1802
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826. **CVE ID : CVE-2023-20686**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1804
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772. **CVE ID : CVE-2023-20687**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1805
Integer Overflow or	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1807
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1809
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1811
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1812
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1813

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt8781wifi					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1814
Product: mt8786					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1816
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1817

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1818
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1819
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT87-200423/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	security-bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1821
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1823
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1825
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1826
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1828
Out-of-bounds Read	06-Apr-2023	4.4	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20665		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1830
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1831
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07628518. **CVE ID : CVE-2023-20676**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1833
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1835
Product: mt8788					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20655		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1837
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1838
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07589148. **CVE ID : CVE-2023-20654**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1840
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1842
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1844
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1845
Use After Free	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1847
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1849
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1850
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1851

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1852
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1853

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1854
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1856
Product: mt8789					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1857
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1858

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1859
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1861
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1863
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1864
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765. **CVE ID : CVE-2023-20662**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1866
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1868
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1869
Integer Overflow or Wraparound	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1871
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1873
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1875
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1876
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt8791					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1878
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1880
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1882
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1883
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1884

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**		
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1885
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt8791t					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1887
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1889
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1890
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07571494; Issue ID: ALPS07571494. **CVE ID : CVE-2023-20656**		
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1892
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1894
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1895
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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 ID : CVE-2023-20663**	bulletin/April-2023	
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1897
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**		
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1899
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1900
Integer Overflow or	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to	https://corp.mediatek.com/product-	H-MED-MT87-200423/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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: ALPS07588383. **CVE ID : CVE-2023-20660**	security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1902
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1904
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20676		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1906
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1907
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1908

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07441821. **CVE ID : CVE-2023-20688**	bulletin/April-2023	
Product: mt8791wifi					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1909
Product: mt8795t					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	bulletin/April -2023	
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April -2023	H-MED-MT87-200423/1911
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April -2023	H-MED-MT87-200423/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628168; Issue ID: ALPS07589144. **CVE ID : CVE-2023-20653**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1913
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1915
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1916
Integer Overflow or Wraparound	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1917

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1918
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20663		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1920
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1921
Out-of-bounds Write	06-Apr-2023	6.7	In audio, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1923
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1925
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1926
Integer Overflow or	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to	https://corp.mediatek.com/product-	H-MED-MT87-200423/1927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			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: ALPS07588383. **CVE ID : CVE-2023-20660**	security-bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1928
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1929

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Product: mt8797					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1930
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135.	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20652		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1932
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1933
Out-of-bounds Write	06-Apr-2023	6.7	In geniezone, there is a possible out of bounds write due to a logic error. This	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20656**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1935
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1937
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1938
Integer Overflow	06-Apr-2023	6.7	In wlan, there is a possible out of	https://corp.mediatek.com	H-MED-MT87-200423/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			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 ID : CVE-2023-20663**	/product-security-bulletin/April-2023	
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1940
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1942
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1944
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1945
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1947
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588569. **CVE ID : CVE-2023-20675**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1949
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1951
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1952
Product: mt8797wifi					
Affected Version(s): -					
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	bulletin/April-2023	
Product: mt8798					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1954
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1956
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1958
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1959
Out-of-bounds Write	06-Apr-2023	6.7	In isp, there is a possible out of bounds write due to	https://corp.mediatek.com/product-	H-MED-MT87-200423/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**	security-bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1961
Integer Overflow or Wraparound	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1963
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1965
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1966
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1967

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1968
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1970
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1971
Concurrent Execution using Shared	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could	https://corp.mediatek.com/product-security-	H-MED-MT87-200423/1972

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1973
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628604; Issue ID: ALPS07628604. **CVE ID : CVE-2023-20665**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1975
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1976

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1977
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1978
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT87-200423/1980
Product: mt8871					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**		
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589135. **CVE ID : CVE-2023-20652**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1982
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1984
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1985
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
Product: mt8891					
Affected Version(s): -					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1987
Out-of-bounds Write	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1989
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1990
Use After Free	06-Apr-2023	6.7	In gz, there is a possible double free	https://corp.mediatek.com	H-MED-MT88-200423/1991

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20664**	/product-security-bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1992
Concurrent Execution using Shared Resource with Improper Synchronization	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1994
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	H-MED-MT88-200423/1995
Vendor: quectel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ag550qcn					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	04-Apr-2023	9.8	OS Command Injection vulnerability in quectel AG550QCN allows attackers to execute arbitrary commands via ql_atfwd. **CVE ID : CVE-2023-26921**	N/A	H-QUE-AG55-200423/1996
Vendor: Samsung					
Product: exynos_1280					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Apr-2023	9.8	An issue was discovered in Samsung Exynos Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments. **CVE ID : CVE-2023-28613**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200423/1997
Product: exynos_2200					
Affected Version(s): -					
Integer Overflow or	04-Apr-2023	9.8	An issue was discovered in Samsung Exynos	https://semiconductor.samsung.com/sup	H-SAM-EXYN-200423/1998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments. **CVE ID : CVE-2023-28613**	port/quality-support/product-security-updates/	
Product: exynos_modem_5300					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Apr-2023	9.8	An issue was discovered in Samsung Exynos Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments. **CVE ID : CVE-2023-28613**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	H-SAM-EXYN-200423/1999
Vendor: Tenda					
Product: ac10					
Affected Version(s): 4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the setSchedWifi function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27012**	N/A	H-TEN-AC10-200423/2000
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the get_parentControl_list_Info function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27013**	N/A	H-TEN-AC10-200423/2001
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_46AC38 function. This vulnerability allows attackers to cause a Denial of Service	N/A	H-TEN-AC10-200423/2002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27014**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_4A75C0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27015**	N/A	H-TEN-AC10-200423/2003
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the R7WebsSecurityHandler function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27016**	N/A	H-TEN-AC10-200423/2004
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack	N/A	H-TEN-AC10-200423/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the sub_45DC58 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27017**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_45EC1C function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27018**	N/A	H-TEN-AC10-200423/2006
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_458FBC function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload.	N/A	H-TEN-AC10-200423/2007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27019		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the saveParentControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27020**	N/A	H-TEN-AC10-200423/2008
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the formSetFirewallCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27021**	N/A	H-TEN-AC10-200423/2009
Product: ac5					
Affected Version(s): 1.0					
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the	N/A	H-TEN-AC5-200423/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fromSetSysTime function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25210**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the R7WebsSecurityHandler function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25211**	N/A	H-TEN-AC5-200423/2011
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromSetWirelessRepeat function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25212**	N/A	H-TEN-AC5-200423/2012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the check_param_changed function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25213**	N/A	H-TEN-AC5-200423/2013
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the setSchedWifi function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25214**	N/A	H-TEN-AC5-200423/2014
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the saveParentControlInfo function. This vulnerability allows attackers to cause a Denial of Service	N/A	H-TEN-AC5-200423/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25215**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the formSetFirewallCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25216**	N/A	H-TEN-AC5-200423/2016
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the formWifiBasicSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25217**	N/A	H-TEN-AC5-200423/2017
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack	N/A	H-TEN-AC5-200423/2018

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the form_fast_setting_wifi_set function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25218**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromDhcpListClient function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25219**	N/A	H-TEN-AC5-200423/2019
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the add_white_node function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload.	N/A	H-TEN-AC5-200423/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25220		
Product: ac6					
Affected Version(s): -					
Out-of-bounds Write	04-Apr-2023	7.5	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-26976**	N/A	H-TEN-AC6-200423/2021
Product: g103					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Apr-2023	9.8	Command injection vulnerability found in Tenda G103 v.1.0.0.5 allows attacker to execute arbitrary code via a the language parameter. **CVE ID : CVE-2023-27076**	N/A	H-TEN-G103-200423/2022
Vendor: totolink					
Product: a7100ru					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Apr-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the org parameter at setting/delStaticDhcpRules.	N/A	H-TOT-A710-200423/2023

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26848		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Apr-2023	9.8	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the pppoeAcName parameter at /setting/setWanIeCfg. **CVE ID : CVE-2023-26978**	N/A	H-TOT-A710-200423/2024
Vendor: toyota					
Product: rav4					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Apr-2023	6.8	Toyota RAV4 2021 vehicles automatically trust messages from other ECUs on a CAN bus, which allows physically proximate attackers to drive a vehicle by accessing the control CAN bus after pulling the bumper away and reaching the headlight connector, and then sending forged "Key is validated" messages via CAN Injection, as exploited in the wild in (for example) July 2022. **CVE ID : CVE-2023-29389**	N/A	H-TOY-RAV4-200423/2025
Operating System					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: AMD					
Product: athlon_gold_3150u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-ATHL-210423/2026
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-ATHL-210423/2027
Product: athlon_silver_3050u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-ATHL-210423/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-ATHL-210423/2029
Product: ryzen_3_2200u_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2030
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2031
Product: ryzen_3_2300u_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2032
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2033
Product: ryzen_3_3200u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2034
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_3_3250u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2036
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2037
Product: ryzen_3_3300u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2039
Product: ryzen_3_3300x_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2040
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_3_3350u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2042
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2043
Product: ryzen_3_3450u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2045
Product: ryzen_3_3500c_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2046
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2047

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_3_3500u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2048
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2049
Product: ryzen_3_3550h_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2051
Product: ryzen_3_3580u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2052
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2053
Product: ryzen_3_3700c_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2054
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2055
Product: ryzen_3_3700u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2056
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_3_3750h_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2058
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2059
Product: ryzen_3_3780u_firmware					
Affected Version(s): -					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2061
Product: ryzen_3_4300ge_firmware					
Affected Version(s): * Up to (excluding) renoirpi-fp6_1.0.0.7					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2062
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_3_4300g_firmware					
Affected Version(s): * Up to (excluding) renoirpi-fp6_1.0.0.7					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2064
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2065
Product: ryzen_3_5125c_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2067
Product: ryzen_3_5300ge_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2068
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_3_5300g_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2070
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2071
Product: ryzen_3_5400u_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2073
Product: ryzen_3_5425c_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2074
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2075
Product: ryzen_3_5425u_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2076
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2077
Product: ryzen_5_2500u_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2078
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_5_2600h_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2080
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2081
Product: ryzen_5_2600x_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2083
Product: ryzen_5_2600_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2084
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_5_2700x_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2086
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2087
Product: ryzen_5_2700_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2089
Product: ryzen_5_3500x_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2090
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2091

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_5_3500_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2092
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2093
Product: ryzen_5_3600xt_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2095
Product: ryzen_5_3600x_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2096
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2097
Product: ryzen_5_3600_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2098
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2099
Product: ryzen_5_4600ge_firmware					
Affected Version(s): * Up to (excluding) renoirpi-fp6_1.0.0.7					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2100
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_5_4600g_firmware					
Affected Version(s): * Up to (excluding) renoirpi-fp6_1.0.0.7					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2102
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2103
Product: ryzen_5_5560u_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2105
Product: ryzen_5_5600ge_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2106
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_5_5600g_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2108
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2109
Product: ryzen_5_5600hs_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2111
Product: ryzen_5_5600h_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2112
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_5_5600u_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2114
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2115
Product: ryzen_5_5625c_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2116

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2117
Product: ryzen_5_5625u_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2118
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2119
Product: ryzen_7_2700u_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2120
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2121
Product: ryzen_7_2700x_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2122
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_7_2700_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2124
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2125
Product: ryzen_7_2800h_firmware					
Affected Version(s): * Up to (excluding) comboam4v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2127
Product: ryzen_7_3700x_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2128
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_7_3800xt_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2130
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2131
Product: ryzen_7_3800x_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2133
Product: ryzen_7_4700ge_firmware					
Affected Version(s): * Up to (excluding) renoirpi-fp6_1.0.0.7					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2134
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2135

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_7_4700g_firmware					
Affected Version(s): * Up to (excluding) renoirpi-fp6_1.0.0.7					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2136
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2137
Product: ryzen_7_5700ge_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2139
Product: ryzen_7_5700g_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2140
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2141
Product: ryzen_7_5800hs_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2142
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2143
Product: ryzen_7_5800h_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2144
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_7_5800u_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2146
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2147
Product: ryzen_7_5825c_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2149
Product: ryzen_7_5825u_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2150
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_9_3900xt_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2152
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2153
Product: ryzen_9_3900x_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2155
Product: ryzen_9_3900_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2156
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_9_3950x_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2158
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2159
Product: ryzen_9_5900hs_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2161
Product: ryzen_9_5900hx_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2162
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2163
Product: ryzen_9_5980hs_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2164
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2165
Product: ryzen_9_5980hx_firmware					
Affected Version(s): * Up to (excluding) cezannepi-fp6_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2166
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2167

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_9_pro_3900_firmware					
Affected Version(s): * Up to (excluding) comboam4_v2_pi_1.2.0.6c					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2168
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2169
Product: ryzen_threadripper_2920x_firmware					
Affected Version(s): * Up to (excluding) summitpi-sp3r2_1.1.0.5					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2171
Product: ryzen_threadripper_2950x_firmware					
Affected Version(s): * Up to (excluding) summitpi-sp3r2_1.1.0.5					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2172
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_threadripper_2970wx_firmware					
Affected Version(s): * Up to (excluding) summitpi-sp3r2_1.1.0.5					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2174
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2175
Product: ryzen_threadripper_2990wx_firmware					
Affected Version(s): * Up to (excluding) summitpi-sp3r2_1.1.0.5					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2177
Product: ryzen_threadripper_3960x_firmware					
Affected Version(s): * Up to (excluding) castlepeakpi-sp3r3_1.0.0.6					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2178
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_threadripper_3970x_firmware					
Affected Version(s): * Up to (excluding) castlepeakpi-sp3r3_1.0.0.6					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2180
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2181
Product: ryzen_threadripper_3990x_firmware					
Affected Version(s): * Up to (excluding) castlepeakpi-sp3r3_1.0.0.6					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20558		
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2183
Product: ryzen_threadripper_pro_3795wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2184
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2185
Product: ryzen_threadripper_pro_3945wx_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2186
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2187
Product: ryzen_threadripper_pro_3955wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2188
N/A	02-Apr-2023	8.8	Insufficient control flow management in	https://www.amd.com/en/	O-AMD-RYZE-210423/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	resources/product-security/bulletin/amd-sb-1027.html	
Product: ryzen_threadripper_pro_3975wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2190
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2191
Product: ryzen_threadripper_pro_3995wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm	https://www.amd.com/en/resources/pro	O-AMD-RYZE-210423/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	duct-security/bulletin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2193
Product: ryzen_threadripper_pro_5945wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2194
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	tin/amd-sb-1027.html	
Product: ryzen_threadripper_pro_5955wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2196
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2197
Product: ryzen_threadripper_pro_5965wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler	https://www.amd.com/en/resources/product-security/bulle	O-AMD-RYZE-210423/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	tin/amd-sb-1027.html	
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2199
Product: ryzen_threadripper_pro_5975wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2200
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges.	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20559		
Product: ryzen_threadripper_pro_5995wx_firmware					
Affected Version(s): * Up to (excluding) castlepeakwspi-swrx8_1.0.0.9					
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmOemSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to an escalation of privileges. **CVE ID : CVE-2023-20558**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2202
N/A	02-Apr-2023	8.8	Insufficient control flow management in AmdCpmGpioInitSmm may allow a privileged attacker to tamper with the SMM handler potentially leading to escalation of privileges. **CVE ID : CVE-2023-20559**	https://www.amd.com/en/resources/product-security/bulletin/amd-sb-1027.html	O-AMD-RYZE-210423/2203
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 15.7.5					
Use After Free	10-Apr-2023	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura	N/A	O-APP-IPAD-210423/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28205**		
Out-of-bounds Write	10-Apr-2023	8.6	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28206**	N/A	O-APP-IPAD-210423/2205
Affected Version(s): From (including) 16.0 Up to (excluding) 16.4.1					
Use After Free	10-Apr-2023	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1,	N/A	O-APP-IPAD-210423/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28205**		
Out-of-bounds Write	10-Apr-2023	8.6	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28206**	N/A	O-APP-IPAD-210423/2207
Product: iphone_os					
Affected Version(s): * Up to (excluding) 15.7.5					
Use After Free	10-Apr-2023	8.8	A use after free issue was addressed with improved memory	N/A	O-APP-IPHO-210423/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28205**		
Out-of-bounds Write	10-Apr-2023	8.6	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28206**	N/A	O-APP-IPHO-210423/2209
Affected Version(s): From (including) 16.0 Up to (excluding) 16.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	10-Apr-2023	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28205**	N/A	O-APP-IPHO-210423/2210
Out-of-bounds Write	10-Apr-2023	8.6	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	N/A	O-APP-IPHO-210423/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28206		
Product: macos					
Affected Version(s): -					
Out-of-bounds Read	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26371**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2212
Out-of-bounds Write	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2023-26372**		
Out-of-bounds Write	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26373**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2214
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26374**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26375**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2216
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26376**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26377**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2218
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26378**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26379**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2220
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26380**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26381**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2222
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26382**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26400**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2224
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26401**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26404**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-APP-MACO-210423/2226
Affected Version(s): * Up to (excluding) 11.7.6					
Out-of-bounds Write	10-Apr-2023	8.6	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	N/A	O-APP-MACO-210423/2227

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28206		
Affected Version(s): * Up to (excluding) 13.3.1					
Use After Free	10-Apr-2023	8.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, Safari 16.4.1, iOS 16.4.1 and iPadOS 16.4.1, macOS Ventura 13.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28205**	N/A	O-APP-MACO-210423/2228
Affected Version(s): From (including) 12.0 Up to (excluding) 12.6.5					
Out-of-bounds Write	10-Apr-2023	8.6	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is	N/A	O-APP-MACO-210423/2229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28206**		
Affected Version(s): From (including) 13.0 Up to (excluding) 13.3.1					
Out-of-bounds Write	10-Apr-2023	8.6	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 15.7.5 and iPadOS 15.7.5, macOS Monterey 12.6.5, iOS 16.4.1 and iPadOS 16.4.1, macOS Big Sur 11.7.6, macOS Ventura 13.3.1. An app may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. **CVE ID : CVE-2023-28206**	N/A	O-APP-MACO-210423/2230
Vendor: Aten					
Product: pe8108_firmware					
Affected Version(s): 2.4.232					
Insufficiently Protected Credentials	11-Apr-2023	7.5	Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. The device allows unauthenticated access to Telnet and SNMP credentials.	https://www.pentagrid.ch/en/blog/multiple-vulnerabilities-in-aten-PE8108-power-	O-ATE-PE81-210423/2231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25413	distribution-unit/	
Insufficiently Protected Credentials	11-Apr-2023	7.2	Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. Restricted users have read access to administrator credentials. **CVE ID : CVE-2023-25407**	https://www.pentagrid.ch/en/blog/multiple-vulnerabilities-in-aten-PE8108-power-distribution-unit/	O-ATE-PE81-210423/2232
N/A	11-Apr-2023	5.3	Aten PE8108 2.4.232 is vulnerable to denial of service (DOS). **CVE ID : CVE-2023-25414**	N/A	O-ATE-PE81-210423/2233
Incorrect Authorization	11-Apr-2023	5.3	Aten PE8108 2.4.232 is vulnerable to Incorrect Access Control. The device allows unauthenticated access to Event Notification configuration. **CVE ID : CVE-2023-25415**	N/A	O-ATE-PE81-210423/2234
Cross-Site Request Forgery (CSRF)	11-Apr-2023	4.3	Aten PE8108 2.4.232 is vulnerable to Cross Site Request Forgery (CSRF). **CVE ID : CVE-2023-25411**	https://www.pentagrid.ch/en/blog/multiple-vulnerabilities-in-aten-PE8108-power-distribution-unit/	O-ATE-PE81-210423/2235
Vendor: Buffalo					
Product: bs-gs2008p_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.0.10.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**	https://www.buffalo.jp/news/detail/20230310-01.html	O-BUF-BS-G-210423/2236
Product: bs-gs2008_firmware					
Affected Version(s): * Up to (including) 1.0.10.01					
Improper Neutralization of	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in	https://www.buffalo.jp/news/detail/202	O-BUF-BS-G-210423/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**	30310-01.html	
Product: bs-gs2016p_firmware					
Affected Version(s): * Up to (including) 1.0.10.01					
Improper Neutralization of Input During Web Page Generation	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console	https://www.buffalo.jp/news/detail/20230310-01.html	O-BUF-BS-G-210423/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2016_firmware					
Affected Version(s): * Up to (including) 1.0.10.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The	https://www.buffalo.jp/news/detail/20230310-01.html	O-BUF-BS-G-210423/2239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2024p_firmware					
Affected Version(s): * Up to (including) 1.0.10.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier,	https://www.buffalo.jp/news/detail/20230310-01.html	O-BUF-BS-G-210423/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2024_firmware					
Affected Version(s): * Up to (including) 1.0.10.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier,	https://www.buffalo.jp/news/detail/20230310-01.html	O-BUF-BS-G-210423/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier, BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Product: bs-gs2048_firmware					
Affected Version(s): * Up to (including) 1.0.10.01					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Apr-2023	5.4	Stored-cross-site scripting vulnerability in Buffalo network devices allows an attacker with access to the web management console of the product to execute arbitrary JavaScript on a legitimate user's web browser. The affected products and versions are as follows: BS-GS2008 firmware Ver. 1.0.10.01 and earlier, BS-GS2016 firmware Ver. 1.0.10.01 and earlier, BS-GS2024 firmware Ver. 1.0.10.01 and earlier, BS-GS2048 firmware Ver. 1.0.10.01 and earlier, BS-GS2008P firmware Ver. 1.0.10.01 and earlier,	https://www.buffalo.jp/news/detail/20230310-01.html	O-BUF-BS-G-210423/2242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BS-GS2016P firmware Ver. 1.0.10.01 and earlier, and BS-GS2024P firmware Ver. 1.0.10.01 and earlier **CVE ID : CVE-2023-24464**		
Vendor: Cisco					
Product: rv016_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	O-CIS-RV01-210423/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access unauthorized data. To exploit this vulnerability, an attacker would need to have valid administrative credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20151**		
Affected Version(s): *					
Improper Neutralization of Input	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	O-CIS-RV01-210423/2248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates that address these vulnerabilities.	/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20137		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-RV01-210423/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20144**	o-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV01-210423/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Product: rv042g_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	O-CIS-RV04-210423/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2261

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	O-CIS-RV04-210423/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates that address these vulnerabilities.	/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20151		
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2265

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management	https://sec.cloudapps.cisco.com/security/center/content	O-CIS-RV04-210423/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities.	/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20143		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Product: rv042_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	O-CIS-RV04-210423/2275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV04-210423/2277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20149**	stored-xss-vqz7gC8W	
Improper Neutralizat	05-Apr-2023	6.1	Multiple vulnerabilities in the	https://sec.cloudapps.cisco.c	O-CIS-RV04-210423/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that address these vulnerabilities. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20151**		
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV04-210423/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20141**	stored-xss-vqz7gC8W	
Improper Neutralizat	05-Apr-2023	6.1	Multiple vulnerabilities in the	https://sec.cloudapps.cisco.c	O-CIS-RV04-210423/2285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that address these vulnerabilities. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV04-210423/2290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Product: rv082_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command	05-Apr-2023	7.2	A vulnerability in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-	O-CIS-RV08-210423/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**	rv01x_rv32x_rce-nzAGWWDD	
Improper Neutralization of Input During	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-RV08-210423/2292

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates that address these vulnerabilities.	Advisory/cisco-sa-rv-stored-xss-vqz7gC8W	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20148		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20151**		
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2297

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-RV08-210423/2299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates that address these vulnerabilities.	Advisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20140		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV08-210423/2305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-RV08-210423/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20147**	o-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rv320_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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 credentials on the affected device. Cisco has not released software updates	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	O-CIS-RV32-210423/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL	O-CIS-RV32-210423/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to have valid Administrator credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. **CVE ID : CVE-2023-20128**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20149**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20151**		
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV32-210423/2313

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20137**	stored-xss-vqz7gC8W	
Improper Neutralizat	05-Apr-2023	6.1	Multiple vulnerabilities in the	https://sec.cloudapps.cisco.c	O-CIS-RV32-210423/2314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			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-based information. Cisco has not released software updates	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that address these vulnerabilities. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20141**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20144**		
Improper Neutralization of	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based	https://sec.cloudapps.cisco.com/security/c	O-CIS-RV32-210423/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')		🟧	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-based information. Cisco has not released software updates that address these vulnerabilities.	enter/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20145		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Affected Version(s): 1.5.1.13					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL	O-CIS-RV32-210423/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. **CVE ID : CVE-2023-20117**		
Product: rv325_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv01x_rv32x_rce-nzAGWWDD	O-CIS-RV32-210423/2325

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates that address this vulnerability. **CVE ID : CVE-2023-20124**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Apr-2023	7.2	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-cmdinject-cKQsZpxL	O-CIS-RV32-210423/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. **CVE ID : CVE-2023-20128**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20148**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV32-210423/2328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20149**	stored-xss-vqz7gC8W	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20150**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20151**		
Affected Version(s): *					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20137**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20138**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20140**		
Improper Neutralization of Input During Web Page Generation	05-Apr-2023	6.1	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-	O-CIS-RV32-210423/2335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20141**	stored-xss-vqz7gC8W	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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-based information. Cisco has not released	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2336

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software updates that address these vulnerabilities. **CVE ID : CVE-2023-20142**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities. **CVE ID : CVE-2023-20143**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2339

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20145**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20146**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Apr-2023	6.1	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)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-stored-xss-vqz7gC8W	O-CIS-RV32-210423/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20147**		
Affected Version(s): 1.5.1.13					
Improper Neutralization of Special Elements used in an OS	05-Apr-2023	7.2	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv32x-	O-CIS-RV32-210423/2342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			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 credentials on the affected device. Cisco has not released software updates to address these vulnerabilities. **CVE ID : CVE-2023-20117**	cmdinject-cKQsZpxL	
Product: rv340w_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.0.03.29					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	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 successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V	O-CIS-RV34-210423/2343
Product: rv340_firmware					
Affected Version(s): * Up to (including) 1.0.03.29					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	A vulnerability in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-	O-CIS-RV34-210423/2344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**	afu-EXxwA65V	
Product: rv345p_firmware					
Affected Version(s): * Up to (including) 1.0.03.29					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V	O-CIS-RV34-210423/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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 successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**		
Product: rv345_firmware					
Affected Version(s): * Up to (including) 1.0.03.29					
Unrestricted Upload of File with Dangerous Type	05-Apr-2023	9.8	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	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V	O-CIS-RV34-210423/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to upload arbitrary files to the affected device. **CVE ID : CVE-2023-20073**		
Product: stealthwatch_management_console_2200_firmware					
Affected Version(s): -					
Deserialization of Untrusted Data	05-Apr-2023	8.8	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 to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the administrator user. **CVE ID : CVE-2023-20102**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealthsmc-rce-sfNBPjcS	O-CIS-STEA-210423/2347
Vendor: Citrix					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: hypervisor					
Affected Version(s): -					
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer handler, where improper privilege management can lead to escalation of privileges and information disclosure. **CVE ID : CVE-2023-0192**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2348
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a memory buffer can lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-0198**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2349
N/A	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in a kernel mode layer handler, which may lead to denial of service or information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0180		
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2351
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of service and data tampering. **CVE ID : CVE-2023-0183**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2352
Incorrect Conversion between Numeric Types	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where sign conversion issuescasting an unsigned primitive to signed may lead to denial of service or information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0185		
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2354
NULL Pointer Dereference	01-Apr-2023	6.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious user in a guest VM can cause a NULL-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2023-0197**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2355
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-CIT-HYPE-210423/2356

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0188		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 12.0					
N/A	06-Apr-2023	6.5	An issue was discovered in libbzip3.a in bzip3 before 1.3.0. A denial of service (process hang) can occur with a crafted archive because bzip3 does not follow the required procedure for interacting with libsais. **CVE ID : CVE-2023-29415**	https://github.com/kspalaiologos/bzip3/issues/95, https://github.com/kspalaiologos/bzip3/compare/1.2.3...1.3.0	O-DEB-DEBI-210423/2357
Vendor: Dell					
Product: emc_powerscale_onefs					
Affected Version(s): 9.5.0.0					
Improper Link Resolution Before File Access ('Link Following')	04-Apr-2023	7.8	Dell PowerScale OneFS version 9.5.0.0 contains improper link resolution before file access vulnerability in isi_gather_info. A low privilege local attacker could potentially exploit this vulnerability, leading to system takeover and it breaks the compliance mode guarantees. **CVE ID : CVE-2023-25940**	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security	O-DEL-EMC_-210423/2358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of a Resource Through its Lifetime	04-Apr-2023	6.5	Dell PowerScale OneFS versions 8.2.x-9.4.x contain an uncontrolled resource consumption vulnerability. A malicious network user with low privileges could potentially exploit this vulnerability in SMB, leading to a potential denial of service. **CVE ID : CVE-2023-25942**	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security	O-DEL-EMC_-210423/2359
Affected Version(s): From (including) 9.1.0.0 Up to (including) 9.1.0.28					
Incorrect Default Permissions	04-Apr-2023	7.8	Dell PowerScale OneFS versions 8.2.x-9.5.0.x contain an elevation of privilege vulnerability. A low-privileged local attacker could potentially exploit this vulnerability, leading to Denial of service, escalation of privileges, and information disclosure. This vulnerability breaks the compliance mode guarantee. **CVE ID : CVE-2023-25941**	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security	O-DEL-EMC_-210423/2360
Improper Control of a Resource Through its Lifetime	04-Apr-2023	6.5	Dell PowerScale OneFS versions 8.2.x-9.4.x contain an uncontrolled resource	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-	O-DEL-EMC_-210423/2361

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consumption vulnerability. A malicious network user with low privileges could potentially exploit this vulnerability in SMB, leading to a potential denial of service. **CVE ID : CVE-2023-25942**	powerscale-onefs-security	
Affected Version(s): From (including) 9.2.1.0 Up to (excluding) 9.2.1.22					
Incorrect Default Permissions	04-Apr-2023	7.8	Dell PowerScale OneFS versions 8.2.x-9.5.0.x contain an elevation of privilege vulnerability. A low-privileged local attacker could potentially exploit this vulnerability, leading to Denial of service, escalation of privileges, and information disclosure. This vulnerability breaks the compliance mode guarantee. **CVE ID : CVE-2023-25941**	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security	O-DEL-EMC_-210423/2362
Improper Control of a Resource Through its Lifetime	04-Apr-2023	6.5	Dell PowerScale OneFS versions 8.2.x-9.4.x contain an uncontrolled resource consumption vulnerability. A malicious network user with low privileges could	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security	O-DEL-EMC_-210423/2363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit this vulnerability in SMB, leading to a potential denial of service. **CVE ID : CVE-2023-25942**		
Affected Version(s): From (including) 9.4.0.0 Up to (excluding) 9.4.0.13					
Incorrect Default Permissions	04-Apr-2023	7.8	Dell PowerScale OneFS versions 8.2.x-9.5.0.x contain an elevation of privilege vulnerability. A low-privileged local attacker could potentially exploit this vulnerability, leading to Denial of service, escalation of privileges, and information disclosure. This vulnerability breaks the compliance mode guarantee. **CVE ID : CVE-2023-25941**	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security	O-DEL-EMC_-210423/2364
Improper Control of a Resource Through its Lifetime	04-Apr-2023	6.5	Dell PowerScale OneFS versions 8.2.x-9.4.x contain an uncontrolled resource consumption vulnerability. A malicious network user with low privileges could potentially exploit this vulnerability in SMB, leading to a potential denial of service.	https://www.dell.com/support/kbdoc/en-us/000211539/dell-emc-powerscale-onefs-security	O-DEL-EMC_-210423/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25942		
Vendor: Dlink					
Product: dir-878_firmware					
Affected Version(s): 1.20b05					
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_475FB0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-24798**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--210423/2366
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_48AF78 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-24799**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--210423/2367
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR878 DIR_878_FW120B05 was discovered to contain a stack overflow in the sub_495220	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--210423/2368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-24800**		
Affected Version(s): 1.30b08					
Out-of-bounds Write	09-Apr-2023	9.8	D-Link DIR878 1.30B08 was discovered to contain a stack overflow in the sub_48d630 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27720**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--210423/2369
Product: dir-882_a1_firmware					
Affected Version(s): 110b02					
Out-of-bounds Write	07-Apr-2023	9.8	D-Link DIR882 DIR882A1_FW110B02 was discovered to contain a stack overflow in the sub_48AC20 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload.	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--210423/2370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24797		
Product: dir878_firmware					
Affected Version(s): 1.30b08					
Out-of-bounds Write	09-Apr-2023	9.8	D-Link DIR878 1.30B08 was discovered to contain a stack overflow in the sub_498308 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27718**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR8-210423/2371
Product: go-rt-ac750_firmware					
Affected Version(s): reva_v101b03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	01-Apr-2023	9.8	D-Link Go-RT-AC750 revA_v101b03 was discovered to contain a command injection vulnerability via the service parameter at soapcgi.main. **CVE ID : CVE-2023-26822**	N/A	O-DLI-GO-R-210423/2372
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 36					
Use After Free	03-Apr-2023	6.3	A use-after-free flaw was found in btrfs_search_slot in fs/btrfs/ctree.c in btrfs in the Linux Kernel.This flaw	https://bugzilla.redhat.com/show_bug.cgi?id=2181342, https://lore.kernel.org/linu	O-FED-FEDO-210423/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to crash the system and possibly cause a kernel information lea **CVE ID : CVE-2023-1611**	x-btrfs/35b9a70650ea947387cf352914a8774b4f7e8a6f.1679481128.git.fdmanana@suse.com/	
Affected Version(s): 37					
Out-of-bounds Write	04-Apr-2023	8.8	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 crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-1810**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2374
Use After Free	04-Apr-2023	8.8	Use after free in Frames 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: High) **CVE ID : CVE-2023-1811**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2375
Improper Restriction	04-Apr-2023	8.8	Out of bounds memory access in	https://chromereleases.goog	O-FED-FEDO-210423/2376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			DOM Bindings in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1812**	leblog.com/2023/04/stable-channel-update-for-desktop.html	
Use After Free	04-Apr-2023	8.8	Use after free in Networking APIs 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: Medium) **CVE ID : CVE-2023-1815**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2377
Use After Free	04-Apr-2023	8.8	Use after free in Vulkan in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1818**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Apr-2023	8.8	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: Medium) **CVE ID : CVE-2023-1820**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2379
N/A	04-Apr-2023	6.5	Inappropriate implementation in Extensions in Google Chrome prior to 112.0.5615.49 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1813**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2380
Improper Input Validation	04-Apr-2023	6.5	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass download checking via a crafted HTML	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1814**		
N/A	04-Apr-2023	6.5	Incorrect security UI in Picture In Picture in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially perform navigation spoofing via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1816**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2382
N/A	04-Apr-2023	6.5	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 security severity: Medium) **CVE ID : CVE-2023-1817**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2383
Out-of-bounds Read	04-Apr-2023	6.5	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	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory read via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-1819**		
N/A	04-Apr-2023	6.5	Inappropriate implementation in WebShare in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1821**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2385
N/A	04-Apr-2023	6.5	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: Low) **CVE ID : CVE-2023-1822**	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2386
N/A	04-Apr-2023	6.5	Inappropriate implementation in FedCM in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass navigation	https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop.html	O-FED-FEDO-210423/2387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restrictions via a crafted HTML page. (Chromium security severity: Low) **CVE ID : CVE-2023-1823**		
Use After Free	03-Apr-2023	6.3	A use-after-free flaw was found in btrfs_search_slot in fs/btrfs/ctree.c in btrfs in the Linux Kernel.This flaw allows an attacker to crash the system and possibly cause a kernel information lea **CVE ID : CVE-2023-1611**	https://bugzilla.redhat.com/show_bug.cgi?id=2181342, https://lore.kernel.org/linux-btrfs/35b9a70650ea947387cf352914a8774b4f7e8a6f.1679481128.git.fdmanana@suse.com/	O-FED-FEDO-210423/2388
Vendor: getnexx					
Product: nxal-100_firmware					
Affected Version(s): * Up to (including) nxal100v-p1-9-1					
Authorization Bypass Through User-Controlled Key	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device settings, and retrieve device information. **CVE ID : CVE-2023-1750**	N/A	O-GET-NXAL-210423/2389
Authorization Bypass Through User-	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An	N/A	O-GET-NXAL-210423/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute. **CVE ID : CVE-2023-1749**		
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	O-GET-NXAL-210423/2391
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated device with only the device's MAC address. **CVE ID : CVE-2023-1752**	N/A	O-GET-NXAL-210423/2392
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials.	N/A	O-GET-NXAL-210423/2393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**		
Product: nxg-100b_firmware					
Affected Version(s): * Up to (including) nxg100bv-p3-4-1					
Authorization Bypass Through User-Controlled Key	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device settings, and retrieve device information. **CVE ID : CVE-2023-1750**	N/A	O-GET-NXG--210423/2394
Authorization Bypass Through User-Controlled Key	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the	N/A	O-GET-NXG--210423/2395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected devices would execute. **CVE ID : CVE-2023-1749**		
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	O-GET-NXG--210423/2396
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated device with only the device's MAC address. **CVE ID : CVE-2023-1752**	N/A	O-GET-NXG--210423/2397
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile	N/A	O-GET-NXG--210423/2398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application or the affected firmware could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**		
Product: nxg-200_firmware					
Affected Version(s): * Up to (including) nxg200v-p3-4-1					
Authorization Bypass Through User-Controlled Key	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device settings, and retrieve device information. **CVE ID : CVE-2023-1750**	N/A	O-GET-NXG--210423/2399
Authorization Bypass Through User-Controlled Key	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute.	N/A	O-GET-NXG--210423/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1749		
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	O-GET-NXG--210423/2401
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated device with only the device's MAC address. **CVE ID : CVE-2023-1752**	N/A	O-GET-NXG--210423/2402
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware	N/A	O-GET-NXG--210423/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could view the credentials and access the MQ Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**		
Product: nxpg-100w_firmware					
Affected Version(s): * Up to (including) nxpg100cv4-0-0					
Authorization Bypass Through User-Controlled Key	04-Apr-2023	7.1	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could retrieve device history, set device settings, and retrieve device information. **CVE ID : CVE-2023-1750**	N/A	O-GET-NXPG-210423/2404
Authorization Bypass Through User-Controlled Key	04-Apr-2023	6.5	The listed versions of Nexx Smart Home devices lack proper access control when executing actions. An attacker with a valid NexxHome deviceId could send API requests that the affected devices would execute. **CVE ID : CVE-2023-1749**	N/A	O-GET-NXPG-210423/2405

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Apr-2023	5.3	The listed versions of Nexx Smart Home devices use a WebSocket server that does not validate if the bearer token in the Authorization header belongs to the device attempting to associate. This could allow any authorized user to receive alarm information and signals meant for other devices which leak a deviceId. **CVE ID : CVE-2023-1751**	N/A	O-GET-NXPG-210423/2406
Improper Authentication	04-Apr-2023	4.3	The listed versions of Nexx Smart Home devices could allow any user to register an already registered alarm or associated device with only the device's MAC address. **CVE ID : CVE-2023-1752**	N/A	O-GET-NXPG-210423/2407
Use of Hard-coded Credentials	04-Apr-2023	10	The listed versions of Nexx Smart Home devices use hard-coded credentials. An attacker with unauthenticated access to the Nexx Home mobile application or the affected firmware could view the credentials and access the MQ	N/A	O-GET-NXPG-210423/2408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Telemetry Server (MQTT) server and the ability to remotely control garage doors or smart plugs for any customer. **CVE ID : CVE-2023-1748**		
Vendor: Google					
Product: android					
Affected Version(s): 12.0					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2409
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2411
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2413
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2414
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2416
Integer Overflow or Wraparound	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2418
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2419
Use After Free	06-Apr-2023	6.7	In gz, there is a possible double free due to a use after free. This could lead	https://corp.mediatek.com/product-security-	O-GOO-ANDR-210423/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2421
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2423
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2425
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2426
Concurrent Execution using Shared Resource with Improper Synchronization	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826. **CVE ID : CVE-2023-20686**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2428
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772. **CVE ID : CVE-2023-20687**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2430
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2431
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2433
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp. mediatek.com /product-security-bulletin/April -2023	O-GOO-ANDR-210423/2435
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp. mediatek.com /product-security-bulletin/April -2023	O-GOO-ANDR-210423/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2437
Affected Version(s): 10.0					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2438
Out-of-bounds Write	06-Apr-2023	6.7	In keyinstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2440
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628168; Issue ID: ALPS07589148. **CVE ID : CVE-2023-20654**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2442
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2443
Use After Free	06-Apr-2023	6.7	In gz, there is a possible double free	https://corp.mediatek.com	O-GOO-ANDR-210423/2444

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20664**	/product-security-bulletin/April-2023	
Affected Version(s): 11.0					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2445
Out-of-bounds Write	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2447
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20654		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2449
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2450
Out-of-bounds Write	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-	O-GOO-ANDR-210423/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**	bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2452
Integer Overflow or Wraparound	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07560765. **CVE ID : CVE-2023-20662**		
Use After Free	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20664**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2454
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2455
Integer Overflow or	06-Apr-2023	6.7	In wlan, there is a possible out of bounds write due to an integer overflow.	https://corp.mediatek.com/product-security-	O-GOO-ANDR-210423/2456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	bulletin/April-2023	
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2457
Out-of-bounds Read	06-Apr-2023	4.4	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2459
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2461
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2462
Out-of-bounds Read	06-Apr-2023	4.4	In power, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441821; Issue ID: ALPS07441821. **CVE ID : CVE-2023-20688**		
Affected Version(s): 13.0					
Improper Privilege Management	06-Apr-2023	7.8	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022. **CVE ID : CVE-2023-20655**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2464
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07628168; Issue ID: ALPS07589135. **CVE ID : CVE-2023-20652**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20653**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2466
Out-of-bounds Write	06-Apr-2023	6.7	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: ALPS07589148. **CVE ID : CVE-2023-20654**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20656**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2468
Out-of-bounds Write	06-Apr-2023	6.7	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485. **CVE ID : CVE-2023-20657**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2469
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07537393; Issue ID: ALPS07180396. **CVE ID : CVE-2023-20658**		
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2471
Integer Overflow or Wraparound	06-Apr-2023	6.7	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07560782. **CVE ID : CVE-2023-20661**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2473
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2474
Use After Free	06-Apr-2023	6.7	In gz, there is a possible double free due to a use after free. This could lead	https://corp.mediatek.com/product-security-	O-GOO-ANDR-210423/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952. **CVE ID : CVE-2023-20664**	bulletin/April-2023	
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20666**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2476
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07648710; Issue ID: ALPS07648710. **CVE ID : CVE-2023-20670**		
N/A	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07664785; Issue ID: ALPS07664785. **CVE ID : CVE-2023-20680**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2478
Out-of-bounds Write	06-Apr-2023	6.7	In adsp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696134; Issue ID: ALPS07696134. **CVE ID : CVE-2023-20681**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2480
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069. **CVE ID : CVE-2023-20684**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2481
Concurrent Execution using Shared Resource with Improper Synchronization	06-Apr-2023	6.4	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2482

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575. **CVE ID : CVE-2023-20685**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826. **CVE ID : CVE-2023-20686**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2483
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-Apr-2023	6.4	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 needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772. **CVE ID : CVE-2023-20687**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2485
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20665**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2486
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07588552. **CVE ID : CVE-2023-20674**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2488
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2490
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07441821. **CVE ID : CVE-2023-20688**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-GOO-ANDR-210423/2492
Vendor: greenpacket					
Product: ot-235_firmware					
Affected Version(s): m-idu-1.6.0.3_v1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2023	9.8	GreenPacket OH736's WR-1200 Indoor Unit, OT-235 with firmware versions M-IDU-1.6.0.3_V1.1 and MH-46360-2.0.3-R5-GP respectively are vulnerable to remote command injection. Commands are executed using pre-login execution and executed with root privileges allowing complete takeover. **CVE ID : CVE-2023-26866**	N/A	O-GRE-OT-2-210423/2493
Affected Version(s): mh-46360-2.0.3-r5-gp					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2023	9.8	GreenPacket OH736's WR-1200 Indoor Unit, OT-235 with firmware versions M-IDU-1.6.0.3_V1.1 and MH-46360-2.0.3-R5-GP respectively are vulnerable to remote command injection. Commands are executed using pre-login execution and executed with root privileges allowing complete takeover. **CVE ID : CVE-2023-26866**	N/A	O-GRE-OT-2-210423/2494
Product: wr-1200_firmware					
Affected Version(s): m-idu-1.6.0.3_v1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	04-Apr-2023	9.8	GreenPacket OH736's WR-1200 Indoor Unit, OT-235 with firmware versions M-IDU-1.6.0.3_V1.1 and MH-46360-2.0.3-R5-GP respectively are vulnerable to remote command injection. Commands are executed using pre-login execution and executed with root privileges allowing complete takeover. **CVE ID : CVE-2023-26866**	N/A	O-GRE-WR-1-210423/2495
Vendor: H3C					
Product: magic_r100_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DelDNSHnList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27801**	N/A	O-H3C-MAGI-210423/2496
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EditvsList parameter at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27802**	N/A	O-H3C-MAGI-210423/2497
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EdittriggerList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload.	N/A	O-H3C-MAGI-210423/2498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27803		
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DelvsList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27804**	N/A	O-H3C-MAGI-210423/2499
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EditSTList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27805**	N/A	O-H3C-MAGI-210423/2500
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the ipqos_lanip_dellist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of	N/A	O-H3C-MAGI-210423/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27806**		
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the Delstlist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27807**	N/A	O-H3C-MAGI-210423/2502
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DeltriggerList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27808**	N/A	O-H3C-MAGI-210423/2503
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the ipqos_lanip_editlist interface at /goform/aspForm. This vulnerability	N/A	O-H3C-MAGI-210423/2504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27810**		
Affected Version(s): v100r005					
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DelDNSHnList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27801**	N/A	O-H3C-MAGI-210423/2505
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EditvsList parameter at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27802**	N/A	O-H3C-MAGI-210423/2506
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EdittriggerList	N/A	O-H3C-MAGI-210423/2507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27803**		
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DelvsList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27804**	N/A	O-H3C-MAGI-210423/2508
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the EditSTList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27805**	N/A	O-H3C-MAGI-210423/2509
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the	N/A	O-H3C-MAGI-210423/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ipqos_lanip_dellist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27806**		
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the Delstlist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27807**	N/A	O-H3C-MAGI-210423/2511
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to contain a stack overflow via the DeltriggerList interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27808**	N/A	O-H3C-MAGI-210423/2512
Out-of-bounds Write	07-Apr-2023	4.9	H3C Magic R100 R100V100R005.bin was discovered to	N/A	O-H3C-MAGI-210423/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the ipqos_lanip_editlist interface at /goform/aspForm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted payload. **CVE ID : CVE-2023-27810**		
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 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 trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248416, https://www.ibm.com/support/pages/node/6964836	O-HP-HP-U-210423/2514
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Improper Neutralization of Input During	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 is vulnerable to cross-site scripting. This vulnerability	https://exchange.xforce.ibmcloud.com/vulnerabilities/248416,	O-IBM-AIX-210423/2515

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	https://www.ibm.com/support/pages/node/6964836	
Product: i					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 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 trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248416, https://www.ibm.com/support/pages/node/6964836	O-IBM-I-210423/2516
Product: z\/os					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to	https://exchange.xforce.ibmcloud.com/vulnerabilities/248416, https://www.i	O-IBM-Z\/O-210423/2517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	bm.com/support/pages/node/6964836	
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer handler which may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering. **CVE ID : CVE-2023-0189**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2518
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a memory buffer can lead to denial of service, information	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure, and data tampering. **CVE ID : CVE-2023-0198**		
N/A	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in a kernel mode layer handler, which may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0180**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2520
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2521
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of service and data tampering.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2522

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0183		
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2523
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA DCGM for Linux contains a vulnerability in HostEngine (server component) where a user may cause a heap-based buffer overflow through the bound socket. A successful exploit of this vulnerability may lead to denial of service and data tampering. **CVE ID : CVE-2023-0208**	https://nvidia.custhelp.com/app/answers/detail/a_id/5453	O-LIN-LINU-210423/2524
Out-of-bounds Write	03-Apr-2023	6.5	A heap-based overflow vulnerability in Trellix Agent (Windows and Linux) version 5.7.8 and earlier, allows a remote user to alter the page heap in the macmnsvc process memory block resulting in the	https://kcm.trellix.com/corporate/index?page=content&id=SB10396	O-LIN-LINU-210423/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service becoming unavailable. **CVE ID : CVE-2023-0977**		
Use After Free	03-Apr-2023	6.3	A use-after-free flaw was found in btrfs_search_slot in fs/btrfs/ctree.c in btrfs in the Linux Kernel.This flaw allows an attacker to crash the system and possibly cause a kernel information lea **CVE ID : CVE-2023-1611**	https://bugzilla.redhat.com/show_bug.cgi?id=2181342, https://lore.kernel.org/linux-btrfs/35b9a70650ea947387cf352914a8774b4f7e8a6f.1679481128.git.fdmanana@suse.com/	O-LIN-LINU-210423/2526
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service. **CVE ID : CVE-2023-0188**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2527
Improper Neutralization of Input During Web Page Generation	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary	https://exchange.xforce.ibmcloud.com/vulnerabilities/248416, https://www.ibm.com/supp	O-LIN-LINU-210423/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	ort/pages/node/6964836	
N/A	01-Apr-2023	4.6	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer driver, where an invalid display configuration may lead to denial of service. **CVE ID : CVE-2023-0194**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-LIN-LINU-210423/2529
Affected Version(s): * Up to (excluding) 5.18_25					
Use After Free	05-Apr-2023	7.1	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 to crash the system, and could even lead to a kernel information leak problem. **CVE ID : CVE-2023-1838**	https://lore.kernel.org/netdev/20220516084213.26854-1-jasowang@redhat.com/T/	O-LIN-LINU-210423/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.7					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	05-Apr-2023	4.7	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. **CVE ID : CVE-2023-1582**	https://lore.kernel.org/linux-mm/Yg6ac8WlwtnDH6M0@kroah.com/	O-LIN-LINU-210423/2531
Affected Version(s): * Up to (excluding) 6.2.8					
N/A	10-Apr-2023	7.8	An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4. **CVE ID : CVE-2023-30456**	https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.2.8	O-LIN-LINU-210423/2532
Affected Version(s): * Up to (excluding) 6.3					
Use After Free	05-Apr-2023	6.3	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 attacker to crash the system due to a race problem.	https://lore.kernel.org/all/20230318122758.2140868-1-linux@roeck-us.net/	O-LIN-LINU-210423/2533

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability could even lead to a kernel information leak problem. **CVE ID : CVE-2023-1855**		
Affected Version(s): 4.19					
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2534
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2536
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2537
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2539
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20674		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2541
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2542
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	O-LIN-LINU-210423/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20677**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-LIN-LINU-210423/2544
Affected Version(s): 5.7					
Concurrent Execution using Shared Resource with Improper Synchronization	05-Apr-2023	4.7	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	https://lore.kernel.org/linux-mm/Yg6ac8WlwtnDH6M0@kroah.com/	O-LIN-LINU-210423/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			user privilege to cause a denial of service. **CVE ID : CVE-2023-1582**		
Affected Version(s): 6.3					
N/A	10-Apr-2023	7.8	An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4. **CVE ID : CVE-2023-30456**	https://cdn.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.2.8	O-LIN-LINU-210423/2546
Use After Free	05-Apr-2023	6.3	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 attacker to crash the system due to a race problem. This vulnerability could even lead to a kernel information leak problem. **CVE ID : CVE-2023-1855**	https://lore.kernel.org/all/20230318122758.2140868-1-linux@roeck-us.net/	O-LIN-LINU-210423/2547
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-0182**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2548
Improper Preservation of Permissions	03-Apr-2023	7.8	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 be executed. This allows the user to elevate their permissions. **CVE ID : CVE-2023-0975**	https://kcm.trellix.com/corporate/index?page=content&id=SB10396	O-MIC-WIND-210423/2549
Out-of-bounds Read	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26371**		
Out-of-bounds Write	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26372**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2551
Out-of-bounds Write	12-Apr-2023	7.8	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26373		
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2553
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an out-of-bounds write can lead to denial of service and data tampering. **CVE ID : CVE-2023-0186**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2554
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	03-Apr-2023	6.5	A heap-based overflow vulnerability in Trellix Agent (Windows and Linux) version 5.7.8 and earlier, allows a remote user to alter the page heap in the macmnsvc process memory block resulting in the service becoming unavailable. **CVE ID : CVE-2023-0977**	https://kcm.trellix.com/corporate/index?page=content&id=SB10396	O-MIC-WIND-210423/2556
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds read can lead to denial of service. **CVE ID : CVE-2023-0187**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2557
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2558

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0188		
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26374**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2559
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26375**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26376**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2561
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26377**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26378**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2563
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26379**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26380**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2565
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26381**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26382**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2567
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26400**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26401**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2569
Out-of-bounds Read	12-Apr-2023	5.5	Adobe Dimension version 3.4.8 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2023-26404**	https://helpx.adobe.com/security/products/dimension/apsb23-27.html	O-MIC-WIND-210423/2570
Improper Neutralization of	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 is vulnerable to	https://exchange.xforce.ibmcloud.com/vul	O-MIC-WIND-210423/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			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 trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	nerabilities/248416, https://www.ibm.com/support/pages/node/6964836	
N/A	01-Apr-2023	4.6	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer driver, where an invalid display configuration may lead to denial of service. **CVE ID : CVE-2023-0194**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2572
Improper Validation of Specified Quantity in Input	01-Apr-2023	2.4	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer driver nvlddmkm.sys, where an can cause CWE-1284, which may lead to hypothetical Information leak of unimportant data such as local variable data of the driver	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-MIC-WIND-210423/2573

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0195		
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.19869					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2574
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2575
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2576
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2577
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24924**	bility/CVE-2023-24924	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2579
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2580
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2581
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2582
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24929**	bility/CVE-2023-24929	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2584
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2585
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2586
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2587
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2588
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2589

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28236	guide/vulnerability/CVE-2023-28236	
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2590
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2591
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2592
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2593
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2594
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2595

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28217	bility/CVE-2023-28217	
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2596
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2597
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2598
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2599
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2600
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28216**	bility/CVE-2023-28216	
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2602
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2603
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2604
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2605
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2606
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability	https://msrc.microsoft.com	O-MIC-WIND-210423/2607

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28228	/update-guide/vulnerability/CVE-2023-28228	
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2608
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2609
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.5850					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2610
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2611
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2612

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24886		
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2613
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2614
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2615
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2616
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2617

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24927		
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2618
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2619
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2620
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2621
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2623
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2624
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2625
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2626
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2627
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2628
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2629

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24885**	bility/CVE-2023-24885	
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2630
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2631
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2632
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2633
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2634
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP)	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	guide/vulnerability/CVE-2023-28241	
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2636
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2637
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2638
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2639
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2640
N/A	11-Apr-2023	5.5	Windows Common Log File System	https://msrc.microsoft.com	O-MIC-WIND-210423/2641

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	/update-guide/vulnerability/CVE-2023-28266	
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2642
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2643
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2644
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2645
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.4252					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2647
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2648
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2649
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2650
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2652
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2653
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2654
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2655
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2657
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2658
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2659
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2660
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2661
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2662
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28252**	guide/vulnerability/CVE-2023-28252	
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2664
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2665
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2666
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2667
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2668
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2669

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-28232**	bility/CVE-2023-28232	
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2670
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2671
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2672
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2673
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2675
N/A	11-Apr-2023	6.8	Windows Lock Screen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28235**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28235	O-MIC-WIND-210423/2676
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2677
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2678
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2679
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2681
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2682
Product: windows_10_20h2					
Affected Version(s): * Up to (excluding) 10.0.19042.2846					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2683
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2684
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2685
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	guide/vulnerability/CVE-2023-24887	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2687
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2688
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2689
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2690
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24928**	bility/CVE-2023-24928	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2692
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2693
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2694
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2695
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2697
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2698
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2699
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2700
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2701
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2703
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2704
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2705
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2706
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2707
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2709
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2710
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2711
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2712
N/A	11-Apr-2023	6.8	Windows Lock Screen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28235**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28235	O-MIC-WIND-210423/2713
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2715
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2716
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2717
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2718
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2719
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.2846					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2720

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2721
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2722
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2723
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2724
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2726
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2727
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2728
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2729
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2731
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2732
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2733
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2734
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2735
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2736
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2737

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28252**	guide/vulnerability/CVE-2023-28252	
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2738
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2739
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2740
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2741
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2742
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-28232**	bility/CVE-2023-28232	
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2744
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2745
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2746
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2747
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2748

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2749
N/A	11-Apr-2023	6.8	Windows Lock Screen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28235**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28235	O-MIC-WIND-210423/2750
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2751
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2752
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2753
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2755
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2756
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.2846					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2757
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2758
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2759
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	guide/vulnerability/CVE-2023-24887	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2761
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2762
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2763
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2764
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24928**	bility/CVE-2023-24928	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2766
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2767
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2768
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2769
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2771
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2772
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2773
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2774
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2775
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2777
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2778
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2779
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2780
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2781
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2783
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2784
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2785
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2786
N/A	11-Apr-2023	6.8	Windows Lock Screen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28235**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28235	O-MIC-WIND-210423/2787
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2788

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2789
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2790
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2791
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2792
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2793
Product: windows_11_21h2					
Affected Version(s): * Up to (excluding) 10.0.22000.1817					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2795
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2796
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2797
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2798
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2799

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2800
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2801
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2802
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2803
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2805
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2806
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2807
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2808
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2809
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2810
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2811

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28252**	guide/vulnerability/CVE-2023-28252	
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2812
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2813
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2814
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2815
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2816
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-28232**	bility/CVE-2023-28232	
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-28233**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28233	O-MIC-WIND-210423/2818
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-28234**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28234	O-MIC-WIND-210423/2819
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2820
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2821
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2822
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2823

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28216**	bility/CVE-2023-28216	
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2824
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2825
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2826
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2827
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2828
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability	https://msrc.microsoft.com	O-MIC-WIND-210423/2829

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28228	/update-guide/vulnerability/CVE-2023-28228	
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2830
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2831
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.1555					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2832
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2833
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2835
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2836
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2837
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2838
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2840
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2841
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2842
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2843
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2844
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability **CVE ID : CVE-2023-28219**	guide/vulnerability/CVE-2023-28219	
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2846
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2847
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2848
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2849
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2850
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2851

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24885**	bility/CVE-2023-24885	
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2852
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2853
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2854
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2855
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-28233**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28233	O-MIC-WIND-210423/2856
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-28234**	https://msrc.microsoft.com/update-guide/vulnerability/	O-MIC-WIND-210423/2857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bility/CVE-2023-28234	
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2858
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2859
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2860
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2861
N/A	11-Apr-2023	7	Win32k Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24914**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24914	O-MIC-WIND-210423/2862
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28216		
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2864
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2865
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2866
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2867
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2868
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2869

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28253	bility/CVE-2023-28253	
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2870
Product: windows_server_2008					
Affected Version(s): -					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2871
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2872
N/A	11-Apr-2023	8.8	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-28240**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28240	O-MIC-WIND-210423/2873
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2874

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2875
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2876
N/A	11-Apr-2023	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28244**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28244	O-MIC-WIND-210423/2877
N/A	11-Apr-2023	8	DHCP Server Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-28231**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28231	O-MIC-WIND-210423/2878
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2879
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2880
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28272	guide/vulnerability/CVE-2023-28272	
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2882
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2883
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2884
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2885
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2886
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2887

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28216	bility/CVE-2023-28216	
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2888
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2889
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2890
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2891
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2892
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2893

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2894
Affected Version(s): r2					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2895
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2896
N/A	11-Apr-2023	8.8	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-28240**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28240	O-MIC-WIND-210423/2897
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2898
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2899

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28219	bility/CVE-2023-28219	
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2900
N/A	11-Apr-2023	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28244**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28244	O-MIC-WIND-210423/2901
N/A	11-Apr-2023	8	DHCP Server Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-28231**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28231	O-MIC-WIND-210423/2902
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2903
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2904
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2906
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2907
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2908
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2909
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2910
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2912
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2913
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2914
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2915
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2916
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2917
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2918

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-28266**	guide/vulnerability/CVE-2023-28266	
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2919
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2920
Product: windows_server_2012					
Affected Version(s): -					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2921
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2922
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24884		
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2924
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2925
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2926
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2927
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24925		
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2929
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2930
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2931
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2932
N/A	11-Apr-2023	8.8	Windows Network Load Balancing Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28240	O-MIC-WIND-210423/2933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28240		
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2934
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2935
N/A	11-Apr-2023	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28244**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28244	O-MIC-WIND-210423/2936
N/A	11-Apr-2023	8	DHCP Server Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-28231**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28231	O-MIC-WIND-210423/2937
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2938
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2939
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code	https://msrc.microsoft.com	O-MIC-WIND-210423/2940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-28237**	/update-guide/vulnerability/CVE-2023-28237	
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/2941
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2942
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2943
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2944
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2945
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/2946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	guide/vulnerability/CVE-2023-28238	
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2947
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2948
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2949
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2950
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2951
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28218**	bility/CVE-2023-28218	
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/2953
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2954
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2955
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2956
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2957
N/A	11-Apr-2023	5.5	Windows Kernel Information	https://msrc.microsoft.com	O-MIC-WIND-210423/2958

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-28253**	/update-guide/vulnerability/CVE-2023-28253	
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/2959
Affected Version(s): r2					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2960
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/2961
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/2962
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24886		
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/2964
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/2965
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/2966
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/2967
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/2968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-24926		
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/2969
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/2970
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/2971
N/A	11-Apr-2023	8.8	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-28240**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28240	O-MIC-WIND-210423/2972
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/2974
N/A	11-Apr-2023	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28244**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28244	O-MIC-WIND-210423/2975
N/A	11-Apr-2023	8	DHCP Server Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-28231**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28231	O-MIC-WIND-210423/2976
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/2977
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/2978
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/2979
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/2980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28252**	bility/CVE-2023-28252	
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/2981
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/2982
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/2983
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/2984
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/2985

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/2986
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/2987
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/2988
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/2989
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/2990
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/2991
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call	https://msrc.microsoft.com	O-MIC-WIND-210423/2992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	/update-guide/vulnerability/CVE-2023-28216	
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/2993
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/2994
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/2995
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/2996
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/2997
N/A	11-Apr-2023	4.4	Windows Group Policy Security	https://msrc.microsoft.com	O-MIC-WIND-210423/2998

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	/update-guide/vulnerability/CVE-2023-28276	
Product: windows_server_2016					
Affected Version(s): -					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability **CVE ID : CVE-2023-28250**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28250	O-MIC-WIND-210423/2999
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/3000
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/3001
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/3002
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24887**	bility/CVE-2023-24887	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/3004
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/3005
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/3006
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/3007
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3008

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24927**	bility/CVE-2023-24927	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/3009
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/3010
N/A	11-Apr-2023	8.8	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-28240**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28240	O-MIC-WIND-210423/3011
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/3012
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Apr-2023	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28244**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28244	O-MIC-WIND-210423/3014
N/A	11-Apr-2023	8	DHCP Server Service Remote Code Execution Vulnerability **CVE ID : CVE-2023-28231**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28231	O-MIC-WIND-210423/3015
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/3016
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/3017
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/3018
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/3019
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28272	bility/CVE-2023-28272	
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24885**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24885	O-MIC-WIND-210423/3021
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/3022
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/3023
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/3024
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/3025
N/A	11-Apr-2023	7.5	Windows Network Address Translation	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/3026

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	guide/vulnerability/CVE-2023-28217	
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/3027
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/3028
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/3029
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/3030
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/3031
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3032

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24883**	bility/CVE-2023-24883	
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/3033
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/3034
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/3035
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/3036
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/3037
Product: windows_server_2019					
Affected Version(s): -					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/3038

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-28250**	guide/vulnerability/CVE-2023-28250	
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/3039
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/3040
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/3041
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/3042
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-28243**	bility/CVE-2023-28243	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24924**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24924	O-MIC-WIND-210423/3044
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/3045
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/3046
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/3047
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24928**	bility/CVE-2023-24928	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24929**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24929	O-MIC-WIND-210423/3049
N/A	11-Apr-2023	8.8	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-28240**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28240	O-MIC-WIND-210423/3050
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/3051
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/3052
N/A	11-Apr-2023	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28244**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28244	O-MIC-WIND-210423/3053
N/A	11-Apr-2023	8	DHCP Server Service Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/3054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-28231**	guide/vulnerability/CVE-2023-28231	
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/3055
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/3056
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/3057
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/3058
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/3059
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24885**	bility/CVE-2023-24885	
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/3061
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/3062
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/3063
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/3064
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/3065
N/A	11-Apr-2023	7.5	Windows Network Address Translation	https://msrc.microsoft.com	O-MIC-WIND-210423/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	/update-guide/vulnerability/CVE-2023-28217	
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/3067
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/3068
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28218**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28218	O-MIC-WIND-210423/3069
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/3070
N/A	11-Apr-2023	6.8	Windows Lock Screen Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28235**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28235	O-MIC-WIND-210423/3071
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability **CVE ID : CVE-2023-24883**	bility/CVE-2023-24883	
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/3073
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/3074
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/3075
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/3076
N/A	11-Apr-2023	4.4	Windows Group Policy Security Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28276	O-MIC-WIND-210423/3077
Product: windows_server_2022					
Affected Version(s): -					
N/A	11-Apr-2023	9.8	Windows Pragmatic General Multicast (PGM) Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-28250**	guide/vulnerability/CVE-2023-28250	
N/A	11-Apr-2023	8.8	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability **CVE ID : CVE-2023-28275**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28275	O-MIC-WIND-210423/3079
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24884**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24884	O-MIC-WIND-210423/3080
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24886**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24886	O-MIC-WIND-210423/3081
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24887**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24887	O-MIC-WIND-210423/3082
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24924**	bility/CVE-2023-24924	
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24925**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24925	O-MIC-WIND-210423/3084
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24926**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24926	O-MIC-WIND-210423/3085
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24927**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24927	O-MIC-WIND-210423/3086
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-24928**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24928	O-MIC-WIND-210423/3087
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24929**	bility/CVE-2023-24929	
N/A	11-Apr-2023	8.8	Windows Network Load Balancing Remote Code Execution Vulnerability **CVE ID : CVE-2023-28240**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28240	O-MIC-WIND-210423/3089
N/A	11-Apr-2023	8.8	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28243**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28243	O-MIC-WIND-210423/3090
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28219**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28219	O-MIC-WIND-210423/3091
N/A	11-Apr-2023	8.1	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28220**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28220	O-MIC-WIND-210423/3092
N/A	11-Apr-2023	8.1	Windows Kerberos Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28244**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28244	O-MIC-WIND-210423/3093
N/A	11-Apr-2023	8	DHCP Server Service Remote Code	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-28231**	guide/vulnerability/CVE-2023-28231	
N/A	11-Apr-2023	7.8	Windows Graphics Component Elevation of Privilege Vulnerability **CVE ID : CVE-2023-24912**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24912	O-MIC-WIND-210423/3095
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28236**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28236	O-MIC-WIND-210423/3096
N/A	11-Apr-2023	7.8	Windows Kernel Remote Code Execution Vulnerability **CVE ID : CVE-2023-28237**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28237	O-MIC-WIND-210423/3097
N/A	11-Apr-2023	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28252**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28252	O-MIC-WIND-210423/3098
N/A	11-Apr-2023	7.8	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28272**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28272	O-MIC-WIND-210423/3099
N/A	11-Apr-2023	7.5	Microsoft PostScript and PCL6 Class Printer Driver Remote Code	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability **CVE ID : CVE-2023-24885**	bility/CVE-2023-24885	
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-24931**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24931	O-MIC-WIND-210423/3101
N/A	11-Apr-2023	7.5	Windows Network Address Translation (NAT) Denial of Service Vulnerability **CVE ID : CVE-2023-28217**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28217	O-MIC-WIND-210423/3102
N/A	11-Apr-2023	7.5	Windows Bluetooth Driver Remote Code Execution Vulnerability **CVE ID : CVE-2023-28227**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28227	O-MIC-WIND-210423/3103
N/A	11-Apr-2023	7.5	Windows Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability **CVE ID : CVE-2023-28232**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28232	O-MIC-WIND-210423/3104
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-28233**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28233	O-MIC-WIND-210423/3105
N/A	11-Apr-2023	7.5	Windows Secure Channel Denial of Service Vulnerability **CVE ID : CVE-2023-28234**	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bility/CVE-2023-28234	
N/A	11-Apr-2023	7.5	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability **CVE ID : CVE-2023-28238**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28238	O-MIC-WIND-210423/3107
N/A	11-Apr-2023	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability **CVE ID : CVE-2023-28241**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28241	O-MIC-WIND-210423/3108
N/A	11-Apr-2023	7.1	Windows Kernel Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28222**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28222	O-MIC-WIND-210423/3109
N/A	11-Apr-2023	7	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28229**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28229	O-MIC-WIND-210423/3110
N/A	11-Apr-2023	7	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability **CVE ID : CVE-2023-28216**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28216	O-MIC-WIND-210423/3111
N/A	11-Apr-2023	7	Windows Ancillary Function Driver for WinSock Elevation of	https://msrc.microsoft.com/update-guide/vulnera	O-MIC-WIND-210423/3112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability **CVE ID : CVE-2023-28218**	bility/CVE-2023-28218	
N/A	11-Apr-2023	6.5	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-24883**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24883	O-MIC-WIND-210423/3113
N/A	11-Apr-2023	5.5	Windows Common Log File System Driver Information Disclosure Vulnerability **CVE ID : CVE-2023-28266**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28266	O-MIC-WIND-210423/3114
N/A	11-Apr-2023	5.5	Windows Kernel Memory Information Disclosure Vulnerability **CVE ID : CVE-2023-28271**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28271	O-MIC-WIND-210423/3115
N/A	11-Apr-2023	5.5	Windows Spoofing Vulnerability **CVE ID : CVE-2023-28228**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28228	O-MIC-WIND-210423/3116
N/A	11-Apr-2023	5.5	Windows Kernel Information Disclosure Vulnerability **CVE ID : CVE-2023-28253**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28253	O-MIC-WIND-210423/3117
N/A	11-Apr-2023	4.4	Windows Group Policy Security	https://msrc.microsoft.com/update-	O-MIC-WIND-210423/3118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability **CVE ID : CVE-2023-28276**	guide/vulnerability/CVE-2023-28276	
Vendor: Openbsd					
Product: openbsd					
Affected Version(s): 7.1					
N/A	04-Apr-2023	7.8	ascii_load_sockaddr in smtpd in OpenBSD before 7.1 errata 024 and 7.2 before errata 020, and OpenSMTPD Portable before 7.0.0-portable commit f748277, can abort upon a connection from a local, scoped IPv6 address. **CVE ID : CVE-2023-29323**	https://ftp.openbsd.org/pub/OpenBSD/patches/7.2/common/020_smtpd.patch.sig, https://ftp.openbsd.org/pub/OpenBSD/patches/7.1/common/024_smtpd.patch.sig, https://github.com/OpenSMTPD/OpenSMTPD/commit/41d0eae481f538956b1f1fbadfb5350434540 61f	O-OPE-OPEN-210423/3119
Affected Version(s): 7.2					
N/A	04-Apr-2023	7.8	ascii_load_sockaddr in smtpd in OpenBSD before 7.1 errata 024 and 7.2 before errata 020, and OpenSMTPD Portable before 7.0.0-portable commit f748277, can abort upon a connection from a	https://ftp.openbsd.org/pub/OpenBSD/patches/7.2/common/020_smtpd.patch.sig, https://ftp.openbsd.org/pub/OpenBSD/patches/7.1/common/024_s	O-OPE-OPEN-210423/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local, scoped IPv6 address. **CVE ID : CVE-2023-29323**	mtpd.patch.sig, https://github.com/OpenSMTPD/OpenSMTPD/commit/41d0eae481f538956b1f1fbadfb535043454061f	
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Apr-2023	5.4	IBM WebSphere Application Server 9.0 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 trusted session. IBM X-Force ID: 248416. **CVE ID : CVE-2023-26283**	https://exchange.xforce.ibmcloud.com/vulnerabilities/248416, https://www.ibm.com/support/pages/node/6964836	O-ORA-SOLA-210423/3121
Vendor: quectel					
Product: ag550qcn_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS	04-Apr-2023	9.8	OS Command Injection vulnerability in quectel AG550QCN allows attackers to execute arbitrary	N/A	O-QUE-AG55-210423/3122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands via ql_atfwd. **CVE ID : CVE-2023-26921**		
Vendor: Redhat					
Product: enterprise_linux_kernel-based_virtual_machine					
Affected Version(s): -					
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer handler, where improper privilege management can lead to escalation of privileges and information disclosure. **CVE ID : CVE-2023-0192**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3123
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a memory buffer can lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-0198**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3124
N/A	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in a	https://nvidia.custhelp.com/app/answers	O-RED-ENTE-210423/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel mode layer handler, which may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0180**	/detail/a_id/5452	
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3126
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of service and data tampering. **CVE ID : CVE-2023-0183**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3127
Incorrect Conversion between Numeric Types	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where sign conversion issuescasting an	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unsigned primitive to signed may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0185**		
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3129
NULL Pointer Dereference	01-Apr-2023	6.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious user in a guest VM can cause a NULL-pointer dereference, which may lead to denial of service. **CVE ID : CVE-2023-0197**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3130
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-RED-ENTE-210423/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service. **CVE ID : CVE-2023-0188**		
Vendor: Samsung					
Product: exynos_1280_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Apr-2023	9.8	An issue was discovered in Samsung Exynos Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments. **CVE ID : CVE-2023-28613**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-210423/3132
Product: exynos_2200_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Apr-2023	9.8	An issue was discovered in Samsung Exynos Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-210423/3133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments. **CVE ID : CVE-2023-28613**		
Product: exynos_modem_5300_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	04-Apr-2023	9.8	An issue was discovered in Samsung Exynos Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments. **CVE ID : CVE-2023-28613**	https://semiconductor.samsung.com/support/quality-support/product-security-updates/	O-SAM-EXYN-210423/3134
Vendor: Tenda					
Product: ac10_firmware					
Affected Version(s): 16.03.10.13_cn					
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the setSchedWifi function. This	N/A	O-TEN-AC10-210423/3135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27012**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the get_parentControl_list_Info function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27013**	N/A	O-TEN-AC10-210423/3136
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_46AC38 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27014**	N/A	O-TEN-AC10-210423/3137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_4A75C0 function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27015**	N/A	O-TEN-AC10-210423/3138
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the R7WebsSecurityHandler function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27016**	N/A	O-TEN-AC10-210423/3139
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_45DC58 function. This vulnerability allows attackers to cause a Denial of Service	N/A	O-TEN-AC10-210423/3140

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27017**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_45EC1C function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27018**	N/A	O-TEN-AC10-210423/3141
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the sub_458FBC function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27019**	N/A	O-TEN-AC10-210423/3142
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack	N/A	O-TEN-AC10-210423/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the saveParentControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27020**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC10 US_AC10V4.0si_V16.03.10.13_cn was discovered to contain a stack overflow via the formSetFirewallCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-27021**	N/A	O-TEN-AC10-210423/3144
Product: ac5_firmware					
Affected Version(s): 15.03.06.28					
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromSetSysTime function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute	N/A	O-TEN-AC5_-210423/3145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code via a crafted payload. **CVE ID : CVE-2023-25210**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the R7WebsSecurityHandler function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25211**	N/A	O-TEN-AC5_-210423/3146
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromSetWirelessRepeat function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25212**	N/A	O-TEN-AC5_-210423/3147
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the	N/A	O-TEN-AC5_-210423/3148

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check_param_changed function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25213**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the setSchedWifi function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25214**	N/A	O-TEN-AC5_-210423/3149
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the saveParentControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25215**	N/A	O-TEN-AC5_-210423/3150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the formSetFirewallCfg function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25216**	N/A	O-TEN-AC5_-210423/3151
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the formWifiBasicSet function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25217**	N/A	O-TEN-AC5_-210423/3152
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the form_fast_setting_wifi_set function. This vulnerability allows attackers to cause a Denial of Service	N/A	O-TEN-AC5_-210423/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25218**		
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the fromDhcpListClient function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25219**	N/A	O-TEN-AC5_-210423/3154
Out-of-bounds Write	07-Apr-2023	9.8	Tenda AC5 US_AC5V1.0RTL_V15.03.06.28 was discovered to contain a stack overflow via the add_white_node function. This vulnerability allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted payload. **CVE ID : CVE-2023-25220**	N/A	O-TEN-AC5_-210423/3155
Product: ac6_firmware					
Affected Version(s): 15.03.05.09					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	04-Apr-2023	7.5	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function. **CVE ID : CVE-2023-26976**	N/A	O-TEN-AC6_-210423/3156
Product: g103_firmware					
Affected Version(s): 1.0.0.5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Apr-2023	9.8	Command injection vulnerability found in Tenda G103 v.1.0.0.5 allows attacker to execute arbitrary code via a the language parameter. **CVE ID : CVE-2023-27076**	N/A	O-TEN-G103-210423/3157
Vendor: totolink					
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-Apr-2023	9.8	TOTOlink A7100RU(V7.4cu.2313_B20191024) was discovered to contain a command injection vulnerability via the org parameter at setting/delStaticDhcpRules. **CVE ID : CVE-2023-26848**	N/A	O-TOT-A710-210423/3158
Improper Neutralization of	07-Apr-2023	9.8	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered	N/A	O-TOT-A710-210423/3159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			to contain a command injection vulnerability via the pppoeAcName parameter at /setting/setWanIeCfg. **CVE ID : CVE-2023-26978**		
Vendor: toyota					
Product: rav4_firmware					
Affected Version(s): 2021					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Apr-2023	6.8	Toyota RAV4 2021 vehicles automatically trust messages from other ECUs on a CAN bus, which allows physically proximate attackers to drive a vehicle by accessing the control CAN bus after pulling the bumper away and reaching the headlight connector, and then sending forged "Key is validated" messages via CAN Injection, as exploited in the wild in (for example) July 2022. **CVE ID : CVE-2023-29389**	N/A	O-TOY-RAV4-210423/3160
Vendor: Veritas					
Product: netbackup_appliance_firmware					
Affected Version(s): 4.1.0.1					
Improper Neutralization of	10-Apr-2023	6.1	Veritas Appliance v4.1.0.1 is affected by Host Header	https://github.com/IthacaLabs/Veritas-	O-VER-NETB-210423/3161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Injection attacks. HTTP host header can be manipulated and cause the application to behave in unexpected ways. Any changes made to the header would just cause the request to be sent to a completely different Domain/IP address. **CVE ID : CVE-2023-26788**	Technologies, https://github.com/IthacaLabs/Veritas-Technologies/blob/main/Veritas%20Appliance%20v4.1.0.1/HHI/HHI_CVE-2023-26788.txt	
Vendor: Vmware					
Product: vsphere					
Affected Version(s): -					
N/A	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer handler, where improper privilege management can lead to escalation of privileges and information disclosure. **CVE ID : CVE-2023-0192**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3162
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Apr-2023	7.8	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where improper restriction of operations within the bounds of a	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory buffer can lead to denial of service, information disclosure, and data tampering. **CVE ID : CVE-2023-0198**		
N/A	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in a kernel mode layer handler, which may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0180**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3164
Incorrect Default Permissions	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in a kernel mode layer handler, where memory permissions are not correctly checked, which may lead to denial of service and data tampering. **CVE ID : CVE-2023-0181**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3165
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer where an out-of-bounds write can lead to denial of	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service and data tampering. **CVE ID : CVE-2023-0183**		
Incorrect Conversion between Numeric Types	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel mode layer, where sign conversion issuescasting an unsigned primitive to signed may lead to denial of service or information disclosure. **CVE ID : CVE-2023-0185**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3167
Out-of-bounds Write	01-Apr-2023	7.1	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an out-of-bounds access may lead to denial of service or data tampering. **CVE ID : CVE-2023-0191**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3168
NULL Pointer Dereference	01-Apr-2023	6.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager, where a malicious user in a guest VM can cause a NULL-pointer dereference, which may lead to denial of service.	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0197		
Out-of-bounds Read	01-Apr-2023	5.5	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer handler, where an unprivileged user can cause improper restriction of operations within the bounds of a memory buffer cause an out-of-bounds read, which may lead to denial of service. **CVE ID : CVE-2023-0188**	https://nvidia.custhelp.com/app/answers/detail/a_id/5452	O-VMW-VSPH-210423/3170
Vendor: yoctoproject					
Product: yocto					
Affected Version(s): 3.1					
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3172
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3173
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741. **CVE ID : CVE-2023-20663**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3175
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3177
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3178
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds check. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588569; Issue ID: ALPS07628518. **CVE ID : CVE-2023-20676**		
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3180
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413;	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**		
Affected Version(s): 3.3					
Out-of-bounds Write	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20659**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3182
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20662**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3184
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3185
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**		
Integer Overflow or Wraparound	06-Apr-2023	4.4	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: ALPS07588383. **CVE ID : CVE-2023-20660**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3187
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20674		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588569. **CVE ID : CVE-2023-20675**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3189
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3190
Out-of-bounds Read	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	O-YOC-YOCT-210423/3191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2023-20677**	bulletin/April-2023	
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3192
Affected Version(s): 4.0					
Out-of-bounds Write	06-Apr-2023	6.7	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	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3193

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588413; Issue ID: ALPS07588413. **CVE ID : CVE-2023-20659**		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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. **CVE ID : CVE-2023-20661**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3194
Integer Overflow or Wraparound	06-Apr-2023	6.7	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.	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20662		
Integer Overflow or Wraparound	06-Apr-2023	6.7	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 ID : CVE-2023-20663**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3196
Integer Overflow or Wraparound	06-Apr-2023	6.7	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: ALPS07441605; Issue ID: ALPS07441605. **CVE ID : CVE-2023-20682**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3197
Integer Overflow or Wraparound	06-Apr-2023	4.4	In wlan, there is a possible out of bounds read due to an integer overflow. This could lead to local information	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383. **CVE ID : CVE-2023-20660**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588552. **CVE ID : CVE-2023-20674**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3199
Out-of-bounds Read	06-Apr-2023	4.4	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;	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07588569. **CVE ID : CVE-2023-20675**		
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07628518. **CVE ID : CVE-2023-20676**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3201
Out-of-bounds Read	06-Apr-2023	4.4	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. **CVE ID : CVE-2023-20677**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-Apr-2023	4.4	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: ALPS07588413; Issue ID: ALPS07588453. **CVE ID : CVE-2023-20679**	https://corp.mediatek.com/product-security-bulletin/April-2023	O-YOC-YOCT-210423/3203