National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
01 - 15 Aug 2022 Vol. 09 No. 15

Table of Content

Vendor	Product	Page Number
mediatek	mt6779	992
	mt6781	993
	mt6785	994
	mt6833	995
	mt6853	1000
	mt6853t	1006
	mt6855	1007
	mt6873	1008
	mt6875	1013
	mt6877	1015
	mt6879	1020
	mt6883	1024
	mt6885	1026
	mt6889	1030
	mt6891	1031
	mt6893	1032
	mt6895	1037
	mt6983	1042
	mt6985	1046
	mt7603	1046
	mt7610	1050
	mt7612	1053
	mt7613	1057
	mt7615	1060
	mt7620	1064
	mt7622	1067
	mt7628	1071
	mt7629	1074
	mt7915	1078
	mt7916	1081
	mt7986	1085
	mt8163	1088

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 2code					
Product: discy					
Affected Version(s): * Up to (excluding) 5.0					
Improper Access Control	08-Aug-2022	6.5	The Discy WordPress theme before 5.0 lacks authorization checks then processing ajax requests to the discy_update_options action, allowing any logged in users (with privileges as low as Subscriber,) to change Theme options by sending a crafted POST request. **CVE ID : CVE-2022-1323**	N/A	A-2CO-DISC-170822/1
Vendor: Accusoft					
Product: imagegear					
Affected Version(s): 20.0					
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Aug-2022	9.8	An out-of-bounds write vulnerability exists in the PSD Header processing memory allocation functionality of Accusoft ImageGear 20.0. A specially-crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	N/A	A-ACC-IMAG-170822/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29465		
Vendor: acrontum					
Product: filesystem-template					
Affected Version(s): * Up to (excluding) 0.0.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-Aug-2022	9.8	The package @acrontum/filesystem-template before 0.0.2 are vulnerable to Arbitrary Command Injection due to the fetchRepo API missing sanitization of the href field of external input. **CVE ID : CVE-2022-21186**	https://security.snyk.io/vuln/SNYK-JS-ACRONTUMFILESYSTEMTEMPLATE-2419071, https://github.com/acrontum/filesystem-template/pull/14/commits/baeb727b60991ad82d9e63ac660883793abc0acc	A-ACR-FILE-170822/3
Vendor: Adobe					
Product: framemaker					
Affected Version(s): * Up to (including) 2019.0.8					
Out-of-bounds Read	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35673**		
Out-of-bounds Read	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35674**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/5
Use After Free	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Use After Free	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2022-35675**		
Heap-based Buffer Overflow	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35676**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/7
Heap-based Buffer Overflow	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2022-35677**		
Out-of-bounds Read	11-Aug-2022	5.5	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34264**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/9
Affected Version(s): From (including) 2020 Up to (including) 2020.0.4					
Out-of-bounds Read	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2022-35673**		
Out-of-bounds Read	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35674**		
Use After Free	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35675**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/12
Heap-based Buffer Overflow	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2022-35676**		
Heap-based Buffer Overflow	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35677**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/14
Out-of-bounds Read	11-Aug-2022	5.5	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	A-ADO-FRAM-170822/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34264**		
Product: illustrator					
Affected Version(s): * Up to (including) 25.4.6					
Out-of-bounds Write	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34260**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/16
Use After Free	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2022-34263**		
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34261**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/18
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34262**		
Affected Version(s): From (including) 26.0 Up to (including) 26.3.1					
Out-of-bounds Write	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34260**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/20
Use After Free	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34263		
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34261**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/22
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	A-ADO-ILLU-170822/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim must open a malicious file. **CVE ID : CVE-2022-34262**		
Product: premiere_elements					
Affected Version(s): * Up to (including) 2020.20					
Uncontrolled Search Path Element	11-Aug-2022	7.8	Adobe Premiere Elements version 2020v20 (and earlier) is affected by an Uncontrolled Search Path Element which could lead to Privilege Escalation. An attacker could leverage this vulnerability to obtain admin using an existing low-privileged user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-34235**	https://helpx.adobe.com/security/products/premiere_elements/apsb22-43.html	A-ADO-PREM-170822/24
Product: web_content_management_core_components					
Affected Version(s): * Up to (including) 2.20.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2022	5.4	Adobe Experience Manager Core Components version 2.20.6 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page,	N/A	A-ADO-WEB_-170822/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires a low author privilege access. **CVE ID : CVE-2022-35697**		
Vendor: aescrypt					
Product: aes_crypt					
Affected Version(s): 3.11					
Improper Authentication	03-Aug-2022	5.5	AES Crypt is a file encryption software for multiple platforms. AES Crypt for Linux built using the source on GitHub and having the version number 3.11 has a vulnerability with respect to reading user-provided passwords and confirmations via command-line prompts. Passwords lengths were not checked before being read. This vulnerability may lead to buffer overruns. This does _not_ affect source code found on aescrypt.com, nor is the vulnerability present when providing a password or a key	https://github.com/paulej/AESCrypt/commit/68761851b595e96c68c3f46bfc21167e72c6a22c, https://github.com/paulej/AESCrypt/security/advisories/GHSA-r7fv-72pg-fwrq	A-AES-AES_-170822/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via the `-p` or `-k` command-line options. The problem was fixed via in commit 68761851b and will be included in release 3.16. Users are advised to upgrade. Users unable to upgrade should us the `-p` or `-k` options to provide a password or key. **CVE ID : CVE-2022-35928**		
Vendor: agentejo					
Product: cockpit					
Affected Version(s): * Up to (excluding) 2.2.0					
Insufficient Session Expiration	08-Aug-2022	9.8	Insufficient Session Expiration in GitHub repository cockpit-hq/cockpit prior to 2.2.0. **CVE ID : CVE-2022-2713**	https://github.com/cockpit-hq/cockpit/commit/dd8d0314912fa6517ebd2cc9939d9fafbe68731b, https://huntr.dev/bounties/3080fc96-75d7-4868-84de-9fc8c9b90290	A-AGE-COCK-170822/27
Vendor: alphaware_-_simple_e-commerce_system_project					
Product: alphaware_-_simple_e-commerce_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation	05-Aug-2022	5.4	A vulnerability, which was classified as problematic, has been found in SourceCodester Alphaware Simple E-Commerce System.	N/A	A-ALP-ALPH-170822/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Affected by this issue is some unknown functionality of the file stockin.php. The manipulation of the argument id with the input '"><script>alert(/xss/)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-205670 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2682**		
Vendor: alphaware_e-commerce_system_project					
Product: alphaware_e-commerce_system					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	05-Aug-2022	8.8	A vulnerability was found in SourceCodester Alphaware Simple E-Commerce System. It has been declared as critical. This vulnerability affects unknown code of the file admin_feature.php of the component Background Management Page. The manipulation leads to unrestricted upload. The attack can be initiated	N/A	A-ALP-ALPH-170822/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. VDB-205666 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2678**		
Vendor: Apache					
Product: avro					
Affected Version(s): * Up to (excluding) 0.14.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	09-Aug-2022	7.5	It is possible to provide data to be read that leads the reader to loop in cycles endlessly, consuming CPU. This issue affects Rust applications using Apache Avro Rust SDK prior to 0.14.0 (previously known as avro-rs). Users should update to apache-avro version 0.14.0 which addresses this issue. **CVE ID : CVE-2022-35724**	https://lists.apache.org/thread/771z1nwrpkn1ovmyfb2fm65mchdxgy7p	A-APA-AVRO-170822/30
Allocation of Resources Without Limits or Throttling	09-Aug-2022	7.5	It is possible for a Reader to consume memory beyond the allowed constraints and thus lead to out of memory on the system. This issue affects Rust applications using Apache Avro Rust SDK prior to 0.14.0 (previously known	https://lists.apache.org/thread/kj429rzo1xxjgz058qqqg0y7c0p512zo	A-APA-AVRO-170822/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as avro-rs). Users should update to apache-avro version 0.14.0 which addresses this issue. **CVE ID : CVE-2022-36124**		
Integer Overflow or Wraparound	09-Aug-2022	7.5	It is possible to crash (panic) an application by providing a corrupted data to be read. This issue affects Rust applications using Apache Avro Rust SDK prior to 0.14.0 (previously known as avro-rs). Users should update to apache-avro version 0.14.0 which addresses this issue. **CVE ID : CVE-2022-36125**	https://lists.apache.org/thread/t1r5xz0pvhm4tosqopjpj6dz8zlsht07	A-APA-AVRO-170822/32
Product: hadoop					
Affected Version(s): From (including) 2.0.0 Up to (including) 2.10.1					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	04-Aug-2022	9.8	Apache Hadoop's FileUtil.unTar(File, File) API does not escape the input file name before being passed to the shell. An attacker can inject arbitrary commands. This is only used in Hadoop 3.3 InMemoryAliasMap.completeBootstrapTransfer, which is only ever run by a local	https://lists.apache.org/thread/mxqnb39jfrwgs3j6phwvlrfq4mlox130	A-APA-HADO-170822/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. It has been used in Hadoop 2.x for yarn localization, which does enable remote code execution. It is used in Apache Spark, from the SQL command ADD ARCHIVE. As the ADD ARCHIVE command adds new binaries to the classpath, being able to execute shell scripts does not confer new permissions to the caller. SPARK-38305. "Check existence of file before untarring/zipping", which is included in 3.3.0, 3.1.4, 3.2.2, prevents shell commands being executed, regardless of which version of the hadoop libraries are in use. Users should upgrade to Apache Hadoop 2.10.2, 3.2.4, 3.3.3 or upper (including HADOOP-18136). **CVE ID : CVE-2022-25168**		
Affected Version(s): From (including) 3.0.0 Up to (including) 3.2.3					
Improper Neutralization of Argument Delimiters	04-Aug-2022	9.8	Apache Hadoop's FileUtil.unTar(File, File) API does not escape the input file name before being	https://lists.apache.org/thread/mxqnb39jfrwgs3j6phwvlrfq4mlox130	A-APA-HADO-170822/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in a Command ('Argument Injection')			passed to the shell. An attacker can inject arbitrary commands. This is only used in Hadoop 3.3 InMemoryAliasMap.completeBootstrapTransfer, which is only ever run by a local user. It has been used in Hadoop 2.x for yarn localization, which does enable remote code execution. It is used in Apache Spark, from the SQL command ADD ARCHIVE. As the ADD ARCHIVE command adds new binaries to the classpath, being able to execute shell scripts does not confer new permissions to the caller. SPARK-38305. "Check existence of file before untarring/zipping", which is included in 3.3.0, 3.1.4, 3.2.2, prevents shell commands being executed, regardless of which version of the hadoop libraries are in use. Users should upgrade to Apache Hadoop 2.10.2, 3.2.4, 3.3.3 or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upper (including HADOOP-18136). **CVE ID : CVE-2022-25168**		
Affected Version(s): From (including) 3.3.0 Up to (including) 3.3.2					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	04-Aug-2022	9.8	Apache Hadoop's FileUtil.unTar(File, File) API does not escape the input file name before being passed to the shell. An attacker can inject arbitrary commands. This is only used in Hadoop 3.3 InMemoryAliasMap.completeBootstrapTransfer, which is only ever run by a local user. It has been used in Hadoop 2.x for yarn localization, which does enable remote code execution. It is used in Apache Spark, from the SQL command ADD ARCHIVE. As the ADD ARCHIVE command adds new binaries to the classpath, being able to execute shell scripts does not confer new permissions to the caller. SPARK-38305. "Check existence of file before untarring/zipping", which is included in	https://lists.apache.org/thread/mxqnb39jfrwgs3j6phwvlrfq4mlox130	A-APA-HADO-170822/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.3.0, 3.1.4, 3.2.2, prevents shell commands being executed, regardless of which version of the hadoop libraries are in use. Users should upgrade to Apache Hadoop 2.10.2, 3.2.4, 3.3.3 or upper (including HADOOP-18136). **CVE ID : CVE-2022-25168**		
Product: jspwiki					
Affected Version(s): * Up to (excluding) 2.11.3					
Cross-Site Request Forgery (CSRF)	04-Aug-2022	8.8	A carefully crafted invocation on the Image plugin could trigger an CSRF vulnerability on Apache JSPWiki before 2.11.3, which could allow a group privilege escalation of the attacker's account. Further examination of this issue established that it could also be used to modify the email associated with the attacked account, and then a reset password request from the login page. **CVE ID : CVE-2022-34158**	https://jspwiki-wiki.apache.org/Wiki.jsp?page=CVE-2022-34158	A-APA-JSPW-170822/36
Cross-Site Request	04-Aug-2022	6.5	A carefully crafted request on UserPreferences.jsp	https://jspwiki-wiki.apache.org	A-APA-JSPW-170822/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			could trigger an CSRF vulnerability on Apache JSPWiki before 2.11.3, which could allow the attacker to modify the email associated with the attacked account, and then a reset password request from the login page. **CVE ID : CVE-2022-28731**	/Wiki.jsp?page=CVE-2022-28732	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2022	6.1	A carefully crafted request on XHRHtml2Markup.jsp could trigger an XSS vulnerability on Apache JSPWiki up to and including 2.11.2, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. **CVE ID : CVE-2022-27166**	https://jspwiki-wiki.apache.org/Wiki.jsp?page=CVE-2022-28732	A-APA-JSPW-170822/38
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2022	6.1	A carefully crafted request on AJAXPreview.jsp could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim.	https://jspwiki-wiki.apache.org/Wiki.jsp?page=CVE-2022-28732	A-APA-JSPW-170822/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability leverages CVE-2021-40369, where the Denounce plugin dangerously renders user-supplied URLs. Upon re-testing CVE-2021-40369, it appears that the patch was incomplete as it was still possible to insert malicious input via the Denounce plugin. Apache JSPWiki users should upgrade to 2.11.3 or later. **CVE ID : CVE-2022-28730**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2022	6.1	A carefully crafted request on WeblogPlugin could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.11.3 or later. **CVE ID : CVE-2022-28732**	https://jspwiki-wiki.apache.org/Wiki.jsp?page=CVE-2022-28732	A-APA-JSPW-170822/40
Product: traffic_server					
Affected Version(s): From (including) 8.0.0 Up to (including) 8.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/2 request validation of Apache Traffic Server allows an attacker to create smuggle or cache poison attacks. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-25763**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/41
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/1.1 header parsing of Apache Traffic Server allows an attacker to send invalid headers. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-28129**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/42
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in handling the Transfer-Encoding header of Apache Traffic Server allows an attacker to poison the cache. This issue affects Apache Traffic Server 8.0.0 to 9.0.2. **CVE ID : CVE-2022-31778**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/2 header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-31779**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/44
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/2 frame handling of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-31780**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/45
Affected Version(s): From (including) 9.0.0 Up to (including) 9.1.2					
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/2 request validation of Apache Traffic Server allows an attacker to create smuggle or cache poison attacks. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-25763**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/1.1 header parsing of Apache Traffic Server allows an attacker to send invalid headers. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-28129**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/47
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in handling the Transfer-Encoding header of Apache Traffic Server allows an attacker to poison the cache. This issue affects Apache Traffic Server 8.0.0 to 9.0.2. **CVE ID : CVE-2022-31778**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/48
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/2 header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-31779**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-Aug-2022	7.5	Improper Input Validation vulnerability in HTTP/2 frame handling of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-31780**	https://lists.apache.org/thread/rc64lwbdgrkv674koc3zl1sljr9vwg21	A-APA-TRAF-170822/50
Vendor: apartment_visitors_management_system_project					
Product: apartment_visitors_management_system					
Affected Version(s): *					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Apartment Visitor Management System and classified as critical. Affected by this issue is some unknown functionality of the file action-visitor.php. The manipulation of the argument editid/remark leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-206168. **CVE ID : CVE-2022-2772**	N/A	A-APA-APAR-170822/51
Improper Neutralization of	11-Aug-2022	6.1	A vulnerability was found in SourceCodester	N/A	A-APA-APAR-170822/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Apartment Visitor Management System. It has been classified as problematic. This affects an unknown part of the file profile.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-206169 was assigned to this vulnerability. **CVE ID : CVE-2022-2773**		
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	9.8	A vulnerability was found in SourceCodester Apartment Visitor Management System 1.0. It has been classified as critical. This affects an unknown part of the file index.php. The manipulation of the argument username with the input ' AND (SELECT 4955 FROM (SELECT(SLEEP(5)))RSzF) AND 'htiy'='htiy 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	N/A	A-APA-APAR-170822/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-205665 was assigned to this vulnerability. **CVE ID : CVE-2022-2677**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	5.4	A vulnerability has been found in SourceCodester Apartment Visitor Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /manage-apartment.php. The manipulation of the argument Apartment Number with the input <script>alert(1)</script> leads to cross site scripting. 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-205672. **CVE ID : CVE-2022-2684**	N/A	A-APA-APAR-170822/54
Vendor: Arista					
Product: cloudvision_portal					
Affected Version(s): From (including) 2020.2.0 Up to (including) 2022.1.0					
Exposure of Sensitive Information to an	05-Aug-2022	5.5	This advisory documents an internally found vulnerability in the on premises deployment model of	https://www.arista.com/en/support/advisories-notices/security-	A-ARI-CLOU-170822/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			Arista CloudVision Portal (CVP) where under a certain set of conditions, user passwords can be leaked in the Audit and System logs. The impact of this vulnerability is that the CVP user login passwords might be leaked to other authenticated users. **CVE ID : CVE-2022-29071**	advisory/15865-security-advisory-0079	
Vendor: ARM					
Product: valhall_gpu_kernel_driver					
Affected Version(s): From (including) r29p0 Up to (including) r38p0					
N/A	02-Aug-2022	5.5	An issue was discovered in the Arm Mali GPU Kernel Driver (Valhall r29p0 through r38p0). A non-privileged user can make improper GPU processing operations to gain access to already freed memory. **CVE ID : CVE-2022-33917**	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities	A-ARM-VALH-170822/56
Vendor: Asustor					
Product: adm					
Affected Version(s): From (including) 3.5.0 Up to (including) 3.5.9.rue3					
Out-of-bounds Write	05-Aug-2022	8.8	A stack-based buffer overflow vulnerability was found inside ADM when using WebDAV due to the lack of	https://www.asustor.com/security/security_advisory_detail?id=12	A-ASU-ADM-170822/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data size validation. An attacker can exploit this vulnerability to run arbitrary code. Affected ADM versions include: 3.5.9.RUE3 and below, 4.0.5.RVI1 and below as well as 4.1.0.RJD1 and below. **CVE ID : CVE-2022-37398**		
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.5.rvi1					
Out-of-bounds Write	05-Aug-2022	8.8	A stack-based buffer overflow vulnerability was found inside ADM when using WebDAV due to the lack of data size validation. An attacker can exploit this vulnerability to run arbitrary code. Affected ADM versions include: 3.5.9.RUE3 and below, 4.0.5.RVI1 and below as well as 4.1.0.RJD1 and below. **CVE ID : CVE-2022-37398**	https://www.asustor.com/security/security_advisory_detail?id=12	A-ASU-ADM-170822/58
Affected Version(s): From (including) 4.1.0 Up to (including) 4.1.0.rjd1					
Out-of-bounds Write	05-Aug-2022	8.8	A stack-based buffer overflow vulnerability was found inside ADM when using WebDAV due to the lack of	https://www.asustor.com/security/security_advisory_detail?id=12	A-ASU-ADM-170822/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data size validation. An attacker can exploit this vulnerability to run arbitrary code. Affected ADM versions include: 3.5.9.RUE3 and below, 4.0.5.RVI1 and below as well as 4.1.0.RJD1 and below. **CVE ID : CVE-2022-37398**		
Vendor: Atlassian					
Product: jira_data_center					
Affected Version(s): * Up to (excluding) 8.13.19					
Improper Control of Generation of Code ('Code Injection')	01-Aug-2022	7.2	This issue exists to document that a security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system administrator permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. In this case the security improvement was to	https://jira.atlassian.com/browse/JRASERVER-73582	A-ATL-JIRA-170822/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protect against using the XStream library to be able to execute arbitrary code in velocity templates. The affected versions are before version 8.13.19, from version 8.14.0 before 8.20.7, and from version 8.21.0 before 8.22.1. **CVE ID : CVE-2022-36799**		
Affected Version(s): * Up to (excluding) 8.20.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2022	6.1	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Reflected Cross-Site Scripting (RXSS) vulnerability in the TeamManagement.jspa endpoint. The affected versions are before version 8.20.8. **CVE ID : CVE-2022-36801**	https://jira.atlassian.com/browse/JRASERVER-73740	A-ATL-JIRA-170822/61
Affected Version(s): From (including) 8.14.0 Up to (excluding) 8.20.7					
Improper Control of Generation of Code ('Code Injection')	01-Aug-2022	7.2	This issue exists to document that a security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server	https://jira.atlassian.com/browse/JRASERVER-73582	A-ATL-JIRA-170822/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Data Center allowed remote attackers with system administrator permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. In this case the security improvement was to protect against using the XStream library to be able to execute arbitrary code in velocity templates. The affected versions are before version 8.13.19, from version 8.14.0 before 8.20.7, and from version 8.21.0 before 8.22.1. **CVE ID : CVE-2022-36799**		
Affected Version(s): From (including) 8.21.0 Up to (excluding) 8.22.1					
Improper Control of Generation of Code ('Code Injection')	01-Aug-2022	7.2	This issue exists to document that a security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system	https://jira.atlassian.com/browse/JRASERVER-73582	A-ATL-JIRA-170822/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. In this case the security improvement was to protect against using the XStream library to be able to execute arbitrary code in velocity templates. The affected versions are before version 8.13.19, from version 8.14.0 before 8.20.7, and from version 8.21.0 before 8.22.1. **CVE ID : CVE-2022-36799**		
Product: jira_server					
Affected Version(s): * Up to (excluding) 8.13.19					
Improper Control of Generation of Code ('Code Injection')	01-Aug-2022	7.2	This issue exists to document that a security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system administrator permissions to execute arbitrary	https://jira.atlassian.com/browse/JRASERVER-73582	A-ATL-JIRA-170822/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. In this case the security improvement was to protect against using the XStream library to be able to execute arbitrary code in velocity templates. The affected versions are before version 8.13.19, from version 8.14.0 before 8.20.7, and from version 8.21.0 before 8.22.1. **CVE ID : CVE-2022-36799**		
Affected Version(s): * Up to (excluding) 8.20.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2022	6.1	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Reflected Cross-Site Scripting (RXSS) vulnerability in the TeamManagement.jspa endpoint. The affected versions are before version 8.20.8. **CVE ID : CVE-2022-36801**	https://jira.atlassian.com/browse/JRASERVER-73740	A-ATL-JIRA-170822/65
Affected Version(s): From (including) 8.14.0 Up to (excluding) 8.20.7					
Improper Control of	01-Aug-2022	7.2	This issue exists to document that a	https://jira.atlassian.com/bro	A-ATL-JIRA-170822/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			security improvement in the way that Jira Server and Data Center use templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system administrator permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. In this case the security improvement was to protect against using the XStream library to be able to execute arbitrary code in velocity templates. The affected versions are before version 8.13.19, from version 8.14.0 before 8.20.7, and from version 8.21.0 before 8.22.1. **CVE ID : CVE-2022-36799**	wse/JRASERVER-73582	
Affected Version(s): From (including) 8.21.0 Up to (excluding) 8.22.1					
Improper Control of Generation of Code ('Code Injection')	01-Aug-2022	7.2	This issue exists to document that a security improvement in the way that Jira Server and Data Center use	https://jira.atlassian.com/browse/JRASERVER-73582	A-ATL-JIRA-170822/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			templates has been implemented. Affected versions of Atlassian Jira Server and Data Center allowed remote attackers with system administrator permissions to execute arbitrary code via Template Injection leading to Remote Code Execution (RCE) in the Email Templates feature. In this case the security improvement was to protect against using the XStream library to be able to execute arbitrary code in velocity templates. The affected versions are before version 8.13.19, from version 8.14.0 before 8.20.7, and from version 8.21.0 before 8.22.1. **CVE ID : CVE-2022-36799**		
Product: jira_service_management					
Affected Version(s): * Up to (excluding) 4.22.2					
Incorrect Authorization	03-Aug-2022	4.3	Affected versions of Atlassian Jira Service Management Server and Data Center allow remote attackers without the "Browse Users" permission to view groups via an	https://jira.atlassian.com/browse/JSDSERVER-11900	A-ATL-JIRA-170822/68

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure vulnerability in the browsegroups.action endpoint. The affected versions are before version 4.22.2. **CVE ID : CVE-2022-36800**		
Vendor: Autodesk					
Product: 3ds_max					
Affected Version(s): From (including) 2020 Up to (excluding) 2020.3.6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Aug-2022	7.8	A Stack-based Buffer Overflow Vulnerability in Autodesk 3ds Max 2022, 2021, and 2020 may lead to code execution through the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer when parsing ActionScript Byte Code files. This vulnerability may allow arbitrary code execution on affected installations of Autodesk 3ds Max. **CVE ID : CVE-2022-25793**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0006	A-AUT-3DS_-170822/69
Affected Version(s): From (including) 2021 Up to (excluding) 2021.3.10					
Buffer Copy without Checking	10-Aug-2022	7.8	A Stack-based Buffer Overflow Vulnerability in Autodesk 3ds Max	https://www.autodesk.com/trust/security-advisories/ads	A-AUT-3DS_-170822/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			2022, 2021, and 2020 may lead to code execution through the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer when parsing ActionScript Byte Code files. This vulnerability may allow arbitrary code execution on affected installations of Autodesk 3ds Max. **CVE ID : CVE-2022-25793**	k-sa-2022-0006	
Affected Version(s): From (including) 2022 Up to (including) 2022.3.3					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	10-Aug-2022	7.8	A Stack-based Buffer Overflow Vulnerability in Autodesk 3ds Max 2022, 2021, and 2020 may lead to code execution through the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer when parsing ActionScript Byte Code files. This vulnerability may allow arbitrary code execution on affected installations of Autodesk 3ds Max.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0006	A-AUT-3DS_-170822/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25793		
Vendor: Automattic					
Product: crowdsignal_dashboard					
Affected Version(s): * Up to (excluding) 3.0.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	6.1	The Crowdsignal Dashboard WordPress plugin before 3.0.8 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting **CVE ID : CVE-2022-2386**	N/A	A-AUT-CROW-170822/72
Vendor: auto_more_tag_project					
Product: auto_more_tag					
Affected Version(s): * Up to (including) 4.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The Auto More Tag WordPress plugin through 4.0.0 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 when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2411**	N/A	A-AUT-AUTO-170822/73
Vendor: backdropcms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: backdrop_cms					
Affected Version(s): * Up to (including) 1.22.0					
Weak Password Recovery Mechanism for Forgotten Password	01-Aug-2022	5.3	An issue in the login and reset password functionality of Backdrop CMS v1.22.0 allows attackers to enumerate usernames via password reset requests and distinct responses returned based on usernames. **CVE ID : CVE-2022-34530**	N/A	A-BAC-BACK-170822/74
Vendor: best_fee_management_system_project					
Product: best_fee_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	9.8	A vulnerability was found in SourceCodester Best Fee Management System. It has been rated as critical. Affected by this issue is the function login of the file admin_class.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-205658 is the identifier assigned to this vulnerability.	N/A	A-BES-BEST-170822/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2674		
Vendor: better_tag_cloud_project					
Product: better_tag_cloud					
Affected Version(s): * Up to (including) 0.99.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The Better Tag Cloud WordPress plugin through 0.99.5 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 when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2412**	N/A	A-BET-BETT-170822/76
Vendor: Bigtreecms					
Product: bigtree_cms					
Affected Version(s): 4.4.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2022	5.4	BigTree CMS 4.4.16 was discovered to contain an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted PDF file. **CVE ID : CVE-2022-36197**	N/A	A-BIG-BIGT-170822/77
Vendor: BMC					
Product: track-it\!					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 20.19.03					
Missing Authentication for Critical Function	03-Aug-2022	9.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of BMC Track-It! 20.21.2.109. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16709. **CVE ID : CVE-2022-35865**	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/78
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	6.5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of BMC Track-It! 20.21.02.109. Authentication is required to exploit this vulnerability. The specific flaw exists within the GetPopupSubQueryDetails endpoint. The	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-16690. **CVE ID : CVE-2022-35864**		
Affected Version(s): 20.20.01					
Missing Authentication for Critical Function	03-Aug-2022	9.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of BMC Track-It! 20.21.2.109. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16709.	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/80

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35865		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	6.5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of BMC Track-It! 20.21.02.109. Authentication is required to exploit this vulnerability. The specific flaw exists within the GetPopupSubQueryDetails endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-16690. **CVE ID : CVE-2022-35864**	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/81
Affected Version(s): 20.20.02					
Missing Authentication for Critical Function	03-Aug-2022	9.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of BMC Track-It! 20.21.2.109. Authentication is not required to exploit	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16709. **CVE ID : CVE-2022-35865**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	6.5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of BMC Track-It! 20.21.02.109. Authentication is required to exploit this vulnerability. The specific flaw exists within the GetPopupSubQueryDetails endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials, leading to further compromise. Was ZDI-CAN-16690. **CVE ID : CVE-2022-35864**		
Affected Version(s): 20.20.03					
Missing Authentication for Critical Function	03-Aug-2022	9.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of BMC Track-It! 20.21.2.109. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16709. **CVE ID : CVE-2022-35865**	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/84
Improper Neutralization of Special Elements used in an SQL Command	03-Aug-2022	6.5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of BMC Track-It! 20.21.02.109.	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Authentication is required to exploit this vulnerability. The specific flaw exists within the GetPopupSubQueryDetails endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-16690. **CVE ID : CVE-2022-35864**		
Affected Version(s): 20.21.01					
Missing Authentication for Critical Function	03-Aug-2022	9.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of BMC Track-It! 20.21.2.109. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16709. **CVE ID : CVE-2022-35865**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	6.5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of BMC Track-It! 20.21.02.109. Authentication is required to exploit this vulnerability. The specific flaw exists within the GetPopupSubQueryDetails endpoint. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-16690. **CVE ID : CVE-2022-35864**	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/87
Affected Version(s): 20.21.02					
Missing Authentica	03-Aug-2022	9.8	This vulnerability allows remote	https://community.bmc.com/s	A-BMC-TRAC-170822/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion for Critical Function			attackers to execute arbitrary code on affected installations of BMC Track-It! 20.21.2.109. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16709. **CVE ID : CVE-2022-35865**	/article/Security-vulnerabilities-patched-in-Track-It-Version-2	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	6.5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of BMC Track-It! 20.21.02.109. Authentication is required to exploit this vulnerability. The specific flaw exists within the GetPopupSubQueryDetails endpoint. The issue results from the lack of proper validation of a user-	https://community.bmc.com/s/article/Security-vulnerabilities-patched-in-Track-It-Version-2	A-BMC-TRAC-170822/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-16690. **CVE ID : CVE-2022-35864**		
Vendor: boltcms					
Product: bolt					
Affected Version(s): * Up to (including) 5.7					
Improper Input Validation	01-Aug-2022	9.1	The foldername parameter in Bolt 5.1.7 was discovered to have incorrect input validation, allowing attackers to perform directory enumeration or cause a Denial of Service (DoS) via a crafted input. **CVE ID : CVE-2022-31321**	N/A	A-BOL-BOLT-170822/90
Vendor: Centreon					
Product: centreon					
Affected Version(s): 21.10.2					
Improper Neutralization of Special Elements used in an SQL Command	03-Aug-2022	7.2	This vulnerability allows remote attackers to escalate privileges on affected installations of Centreon. Authentication is required to exploit this vulnerability.	https://docs.centreon.com/docs/21.10/releases/centreon-core/	A-CEN-CENT-170822/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			The specific flaw exists within the configuration of poller resources. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to escalate privileges to the level of an administrator. Was ZDI-CAN-16335. **CVE ID : CVE-2022-34871**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	6.5	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Centreon. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of Virtual Metrics. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose stored credentials, leading	https://docs.centreon.com/docs/21.10/releases/centreon-core/	A-CEN-CENT-170822/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to further compromise. Was ZDI-CAN-16336. **CVE ID : CVE-2022-34872**		
Vendor: church_management_system_project					
Product: church_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	8.8	A vulnerability classified as critical has been found in SourceCodester Church Management System 1.0. Affected is an unknown function of the file /login.php. The manipulation of the argument username with the input ' OR (SELECT 7064 FROM(SELECT COUNT(*),CONCAT(0x71627a7671,(SELECT (ELT(7064=7064,1))),0x716b707871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jURL 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-205668.	N/A	A-CHU-CHUR-170822/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2680		
Vendor: Cisco					
Product: adaptive_security_appliance_software					
Affected Version(s): * Up to (excluding) 9.17\\(1\\)					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	10-Aug-2022	6.1	A vulnerability in the Clientless SSL VPN (WebVPN) component of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct browser-based attacks. This vulnerability is due to improper validation of input that is passed to the Clientless SSL VPN component. An attacker could exploit this vulnerability by convincing a targeted user to visit a website that can pass malicious requests to an ASA device that has the Clientless SSL VPN feature enabled. A successful exploit could allow the attacker to conduct browser-based attacks, including cross-site scripting attacks, against the targeted user.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-webvpn-LOeKsNmO	A-CIS-ADAP-170822/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20713		
Affected Version(s): From (including) 9.16.0 Up to (excluding) 9.16.3.19					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	A-CIS-ADAP-170822/95

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Affected Version(s): From (including) 9.17.0 Up to (excluding) 9.17.1.13					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	A-CIS-ADAP-170822/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Affected Version(s): From (including) 9.18.0 Up to (excluding) 9.18.2					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive	https://tools.cisco.com/security/center/content/CiscoSecur	A-CIS-ADAP-170822/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to	ityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: broadworks					
Affected Version(s): From (including) 22.0 Up to (excluding) 22.0.2022.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2022	6.1	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-xbhfr4cD	A-CIS-BROA-170822/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2022-20869**		
Affected Version(s): From (including) 23.0 Up to (excluding) 23.0.2022.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2022	6.1	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-xbhfr4cD	A-CIS-BROA-170822/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser-based information. **CVE ID : CVE-2022-20869**		
Affected Version(s): From (including) 24.0 Up to (excluding) 24.0.2022.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-2022	6.1	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. 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. **CVE ID : CVE-2022-20869**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-xbhfr4cD	A-CIS-BROA-170822/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: firepower_threat_defense					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.4					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	A-CIS-FIRE-170822/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Affected Version(s): From (including) 7.1.0 Up to (excluding) 7.2.0.1					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	A-CIS-FIRE-170822/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: identity_services_engine					
Affected Version(s): 2.6.0					
Insufficiently	10-Aug-2022	4.9	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity	https://tools.cisco.com/security/center/content/CiscoSecur	A-CIS-IDEN-170822/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Services Engine (ISE) Software could allow an authenticated, remote attacker to obtain sensitive information. This vulnerability is due to excessive verbosity in a specific REST API output. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain sensitive information, including administrative credentials for an external authentication server. Note: To successfully exploit this vulnerability, the attacker must have valid ERS administrative credentials. **CVE ID : CVE-2022-20914**	ityAdvisory/cisco-sa-ise-pwd-WH64AhQF	
Affected Version(s): 2.7.0					
Insufficiently Protected Credentials	10-Aug-2022	4.9	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-pwd-WH64AhQF	A-CIS-IDEN-170822/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to obtain sensitive information. This vulnerability is due to excessive verbosity in a specific REST API output. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain sensitive information, including administrative credentials for an external authentication server. Note: To successfully exploit this vulnerability, the attacker must have valid ERS administrative credentials. **CVE ID : CVE-2022-20914**		
Affected Version(s): 3.0.0					
Insufficiently Protected Credentials	10-Aug-2022	4.9	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to obtain sensitive information. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-pwd-WH64AhQF	A-CIS-IDEN-170822/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to excessive verbosity in a specific REST API output. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain sensitive information, including administrative credentials for an external authentication server. Note: To successfully exploit this vulnerability, the attacker must have valid ERS administrative credentials. **CVE ID : CVE-2022-20914**		
Affected Version(s): 3.1					
Insufficiently Protected Credentials	10-Aug-2022	4.9	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to obtain sensitive information. This vulnerability is due to excessive verbosity in a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-pwd-WH64AhQF	A-CIS-IDEN-170822/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific REST API output. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain sensitive information, including administrative credentials for an external authentication server. Note: To successfully exploit this vulnerability, the attacker must have valid ERS administrative credentials. **CVE ID : CVE-2022-20914**		
Affected Version(s): From (including) 2.4.0 Up to (excluding) 2.6.0					
Insufficiently Protected Credentials	10-Aug-2022	4.9	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to obtain sensitive information. This vulnerability is due to excessive verbosity in a specific REST API output. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-pwd-WH64AhQF	A-CIS-IDEN-170822/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain sensitive information, including administrative credentials for an external authentication server. Note: To successfully exploit this vulnerability, the attacker must have valid ERS administrative credentials. **CVE ID : CVE-2022-20914**		
Product: unified_communications_manager					
Affected Version(s): From (including) 11.5\\(1\\) Up to (excluding) 14su2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Aug-2022	8.1	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to delete arbitrary files from an affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-file-delete-N2VPmOnE	A-CIS-UNIF-170822/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. This vulnerability exists because the affected software does not properly validate HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow the attacker to delete arbitrary files from the affected system. **CVE ID : CVE-2022-20816**		
Product: webex_meetings					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	6.5	Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow a remote attacker to conduct a cross-site scripting (XSS) attack or a frame hijacking attack against a user of the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20852**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-frmhijck-kO3wmkuS	A-CIS-WEBE-170822/109
Improper Neutralizat	10-Aug-2022	5.4	Multiple vulnerabilities in the	https://tools.cisco.com/securi	A-CIS-WEBE-170822/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			web interface of Cisco Webex Meetings could allow a remote attacker to conduct a cross-site scripting (XSS) attack or a frame hijacking attack against a user of the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20820**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-frmhijck-kO3wmkuS	
Vendor: Ckeditor					
Product: ckeditor5-html-embed					
Affected Version(s): * Up to (excluding) 35.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2022	4.7	CKEditor 5 is a JavaScript rich text editor. A cross-site scripting vulnerability has been discovered affecting three optional CKEditor 5's packages in versions prior to 35.0.1. The vulnerability allowed to trigger a JavaScript code after fulfilling special conditions. The affected packages are `@ckeditor/ckeditor5-markdown-gfm`, `@ckeditor/ckeditor5-html-support`, and `@ckeditor/ckeditor	https://github.com/ckeditor/ckeditor5/security/advisories/GHSA-42wq-rch8-6f6j, https://ckeditor.com/docs/ckeditor5/latest/features/markdown.html, https://ckeditor.com/docs/ckeditor5/latest/features/html-embed.html	A-CKE-CKED-170822/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5-html-embed`. The specific conditions are 1) Using one of the affected packages. In case of `ckeditor5-html-support` and `ckeditor5-html-embed`, additionally, it was required to use a configuration that allows unsafe markup inside the editor. 2) Destroying the editor instance and 3) Initializing the editor on an element and using an element other than `<textarea>` as a base. The root cause of the issue was a mechanism responsible for updating the source element with the markup coming from the CKEditor 5 data pipeline after destroying the editor. This vulnerability might affect a small percent of integrators that depend on dynamic editor initialization/destroy and use Markdown, General HTML Support or HTML embed features. The problem has been recognized and patched. The fix is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			available in version 35.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31175**		
Product: ckeditor5-html-support					
Affected Version(s): * Up to (excluding) 35.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-2022	4.7	CKEditor 5 is a JavaScript rich text editor. A cross-site scripting vulnerability has been discovered affecting three optional CKEditor 5's packages in versions prior to 35.0.1. The vulnerability allowed to trigger a JavaScript code after fulfilling special conditions. The affected packages are `@ckeditor/ckeditor5-markdown-gfm`, `@ckeditor/ckeditor5-html-support`, and `@ckeditor/ckeditor5-html-embed`. The specific conditions are 1) Using one of the affected packages. In case of `ckeditor5-html-support` and `ckeditor5-html-embed`, additionally, it was required to use a configuration that allows unsafe markup inside the	https://github.com/ckeditor/ckeditor5/security/advisories/GHSA-42wq-rch8-6f6j, https://ckeditor.com/docs/ckeditor5/latest/features/markdown.html, https://ckeditor.com/docs/ckeditor5/latest/features/html-embed.html	A-CKE-CKED-170822/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			editor. 2) Destroying the editor instance and 3) Initializing the editor on an element and using an element other than `<textarea>` as a base. The root cause of the issue was a mechanism responsible for updating the source element with the markup coming from the CKEditor 5 data pipeline after destroying the editor. This vulnerability might affect a small percent of integrators that depend on dynamic editor initialization/destroy and use Markdown, General HTML Support or HTML embed features. The problem has been recognized and patched. The fix is available in version 35.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31175**		
Product: ckeditor5-markdown-gfm					
Affected Version(s): * Up to (excluding) 35.0.1					
Improper Neutralization of Input	03-Aug-2022	4.7	CKEditor 5 is a JavaScript rich text editor. A cross-site scripting	https://github.com/ckeditor/ckeditor5/security/advisories	A-CKE-CKED-170822/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability has been discovered affecting three optional CKEditor 5's packages in versions prior to 35.0.1. The vulnerability allowed to trigger a JavaScript code after fulfilling special conditions. The affected packages are `@ckeditor/ckeditor5-markdown-gfm`, `@ckeditor/ckeditor5-html-support`, and `@ckeditor/ckeditor5-html-embed`. The specific conditions are 1) Using one of the affected packages. In case of `ckeditor5-html-support` and `ckeditor5-html-embed`, additionally, it was required to use a configuration that allows unsafe markup inside the editor. 2) Destroying the editor instance and 3) Initializing the editor on an element and using an element other than `<textarea>` as a base. The root cause of the issue was a mechanism responsible for updating the source element with the	/GHSA-42wq-rch8-6f6j, https://ckeditor.com/docs/ckeditor5/latest/features/markdown.html, https://ckeditor.com/docs/ckeditor5/latest/features/html-embed.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			markup coming from the CKEditor 5 data pipeline after destroying the editor. This vulnerability might affect a small percent of integrators that depend on dynamic editor initialization/destroy and use Markdown, General HTML Support or HTML embed features. The problem has been recognized and patched. The fix is available in version 35.0.1. There are no known workarounds for this issue. **CVE ID : CVE-2022-31175**		
Vendor: Clamav					
Product: clamav					
Affected Version(s): * Up to (including) 0.103.5					
Out-of-bounds Write	10-Aug-2022	7.8	A vulnerability in the regex module used by the signature database load module of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an authenticated, local attacker to crash ClamAV at database load time, and	https://blog.clamav.net/2022/05/clamav-01050-01043-01036-released.html	A-CLA-CLAM-170822/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possibly gain code execution. The vulnerability is due to improper bounds checking that may result in a multi-byte heap buffer overwflow write. An attacker could exploit this vulnerability by placing a crafted CDB ClamAV signature database file in the ClamAV database directory. An exploit could allow the attacker to run code as the clamav user. **CVE ID : CVE-2022-20792**		
Affected Version(s): From (including) 0.104.0 Up to (including) 0.104.2					
Out-of-bounds Write	10-Aug-2022	7.8	A vulnerability in the regex module used by the signature database load module of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an authenticated, local attacker to crash ClamAV at database load time, and possibly gain code execution. The vulnerability is due to improper bounds checking that may result in a multi-byte	https://blog.clamav.net/2022/05/clamav-01050-01043-01036-released.html	A-CLA-CLAM-170822/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap buffer overwflow write. An attacker could exploit this vulnerability by placing a crafted CDB ClamAV signature database file in the ClamAV database directory. An exploit could allow the attacker to run code as the clamav user. **CVE ID : CVE-2022-20792**		
Vendor: clinic\'s_patient_management_system_project					
Product: clinic\'s_patient_management_system					
Affected Version(s): 1.0					
N/A	10-Aug-2022	9.8	Clinic's Patient Management System v1.0 has arbitrary code execution via url: ip/pms/users.php. **CVE ID : CVE-2022-36270**	N/A	A-CLI-CLIN-170822/116
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Aug-2022	9.8	Clinic's Patient Management System v1.0 is vulnerable to SQL injection via /pms/update_user.php?id=. **CVE ID : CVE-2022-36750**	N/A	A-CLI-CLIN-170822/117
Vendor: company_website\/cms_project					
Product: company_website\/cms					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	08-Aug-2022	6.5	A vulnerability was found in SourceCodester Company Website CMS and classified as critical. Affected by this issue is some unknown functionality of the file site-settings.php of the component Cookie Handler. The manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-205826 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2702**	N/A	A-COM-COMP-170822/118
Vendor: company_website_cms_project					
Product: company_website_cms					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Company Website CMS. It has been classified as critical. This affects an unknown part of the file /dashboard/updatelogo.php of the component Background Upload Logo Icon. The	N/A	A-COM-COMP-170822/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument xfile/ufile leads to unrestricted upload. It is possible to initiate the attack remotely. The identifier VDB-205881 was assigned to this vulnerability. **CVE ID : CVE-2022-2736**		
Unrestricted Upload of File with Dangerous Type	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Company Website CMS. It has been declared as critical. This vulnerability affects unknown code of the file /dashboard/add-blog.php of the component Add Blog. The manipulation of the argument ufile leads to unrestricted upload. The attack can be initiated remotely. VDB-205882 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2740**	N/A	A-COM-COMP-170822/120
Unrestricted Upload of File with Dangerous Type	11-Aug-2022	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Company Website CMS. Affected is an unknown function of the file	N/A	A-COM-COMP-170822/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/dashboard/add-service.php of the component Add Service Handler. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. VDB-206022 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2750**		
Unrestricted Upload of File with Dangerous Type	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Company Website CMS and classified as critical. Affected by this issue is some unknown functionality of the file /dashboard/add-portfolio.php. The manipulation of the argument ufile leads to unrestricted upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-206024. **CVE ID : CVE-2022-2751**	N/A	A-COM-COMP-170822/122
Unrestricted Upload of File with Dangerous Type	06-Aug-2022	8.8	A vulnerability was found in SourceCodester Company Website CMS and classified as critical. This issue affects some	N/A	A-COM-COMP-170822/123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown processing. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205817 was assigned to this vulnerability. **CVE ID : CVE-2022-2694**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2022	6.1	A vulnerability was found in SourceCodester Company Website CMS. It has been rated as problematic. Affected by this issue is some unknown functionality of the file add-blog.php. The manipulation leads to cross site scripting. The attack may be launched remotely. VDB-205838 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2725**	N/A	A-COM-COMP-170822/124
Affected Version(s): 1.0					
Improper Authentication	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Company Website CMS 1.0. It has been declared as critical.	N/A	A-COM-COMP-170822/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected by this vulnerability is an unknown functionality of the file /dashboard/settings. The manipulation leads to improper authentication. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206161 was assigned to this vulnerability. **CVE ID : CVE-2022-2765**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-2022	5.4	A vulnerability, which was classified as problematic, has been found in SourceCodester Company Website CMS. This issue affects some unknown processing of the file /dashboard/contact. The manipulation of the argument phone 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-206165 was	N/A	A-COM-COMP-170822/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2022-2769**		
Vendor: complete_online_job_search_system_project					
Product: complete_online_job_search_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	4.8	Complete Online Job Search System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the CATEGORY parameter at /category/controller.php?action=edit. **CVE ID : CVE-2022-35162**	N/A	A-COM-COMP-170822/127
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	4.8	Complete Online Job Search System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the U_NAME parameter at /category/controller.php?action=edit. **CVE ID : CVE-2022-35163**	N/A	A-COM-COMP-170822/128
Vendor: crowcpp					
Product: crow					
Affected Version(s): * Up to (excluding) 1.0\\+4					
Off-by-one Error	04-Aug-2022	9.8	Crow before 1.0+4 has a heap-based buffer overflow via the function qs_parse in query_string.h. On successful	https://github.com/CrowCpp/Crow/pull/486	A-CRO-CROW-170822/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation this vulnerability allows attackers to remotely execute arbitrary code in the context of the vulnerable service. **CVE ID : CVE-2022-34970**		
Vendor: crowdfavorite					
Product: progressive_license					
Affected Version(s): * Up to (including) 1.1.0					
Cross-Site Request Forgery (CSRF)	01-Aug-2022	5.4	The Progressive License WordPress plugin through 1.1.0 is lacking any CSRF check when saving its settings, which could allow attackers to make a logged in admin change them. Furthermore, as the plugin allows arbitrary HTML to be inserted in one of the settings, this could lead to Stored XSS issue which will be triggered in the frontend as well. **CVE ID : CVE-2022-2171**	N/A	A-CRO-PROG-170822/130
Vendor: crypto					
Product: cronos					
Affected Version(s): * Up to (including) 0.7.0					
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.3	Ethermint is an Ethereum library. In Ethermint running versions before `v0.17.2`, the contract	https://github.com/evmos/ethermint/commit/144741832007a26dbe950512acbda4ed95	A-CRY-CRON-170822/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`selfdestruct` invocation permanently removes the corresponding bytecode from the internal database storage. However, due to a bug in the `DeleteAccount`function, all contracts that used the identical bytecode (i.e shared the same `CodeHash`) will also stop working once one contract invokes `selfdestruct`, even though the other contracts did not invoke the `selfdestruct` OPCODE. This vulnerability has been patched in Ethermint version v0.18.0. The patch has state machine-breaking changes for applications using Ethermint, so a coordinated upgrade procedure is required. A workaround is available. If a contract is subject to DoS due to this issue, the user can redeploy the same contract, i.e. with identical bytecode, so that the original contract's code is	b2a451, https://github.com/evmos/ethermint/security/advisories/GHSA-f92v-grc2-w2fg	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recovered. The new contract deployment restores the `bytecode hash -> bytecode` entry in the internal state. **CVE ID : CVE-2022-35936**		
Vendor: cvat					
Product: cvat					
Affected Version(s): * Up to (excluding) 2.0.0					
Server-Side Request Forgery (SSRF)	01-Aug-2022	9.8	CVAT is an opensource interactive video and image annotation tool for computer vision. Versions prior to 2.0.0 were found to be subject to a Server-side request forgery (SSRF) vulnerability. Validation has been added to urls used in the affected code path in version 2.0.0. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31188**	https://github.com/cvat-ai/cvat/commit/6fad1764efd922d99dbcda28c4ee72d071aa5a07, https://github.com/cvat-ai/cvat/security/advisories/GHSA-7vpj-j5xv-29pr	A-CVA-CVAT-170822/132
Vendor: Dell					
Product: wyse_management_suite					
Affected Version(s): * Up to (excluding) 3.8.0					
Cleartext Storage of Sensitive	10-Aug-2022	8.8	Dell Wyse Management Suite 3.6.1 and below contains an Plain-text Password	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-	A-DEL-WYSE-170822/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			Storage Vulnerability in UI. An attacker with low privileges could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account. **CVE ID : CVE-2022-33928**	134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	
Generation of Error Message Containing Sensitive Information	10-Aug-2022	7.5	Dell Wyse Management Suite 3.6.1 and below contains Information Disclosure in Devices error pages. An attacker could potentially exploit this vulnerability, leading to the disclosure of certain sensitive information. The attacker may be able to use the exposed information to access and further vulnerability research. **CVE ID : CVE-2022-33930**	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	A-DEL-WYSE-170822/134
Cleartext Storage of Sensitive	10-Aug-2022	6.5	Dell Wyse Management Suite 3.6.1 and below	https://www.dell.com/support/kbdoc/en-	A-DEL-WYSE-170822/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			contains a Sensitive Data Exposure vulnerability. A low privileged malicious user could potentially exploit this vulnerability in order to obtain credentials. The attacker may be able to use the exposed credentials to access the target device and perform unauthorized actions. **CVE ID : CVE-2022-29090**	us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	
N/A	10-Aug-2022	6.5	Dell Wyse Management Suite 3.6.1 and below contains an Improper Access control vulnerability in UI. An remote authenticated attacker could potentially exploit this vulnerability by bypassing access controls in order to download reports containing sensitive information. **CVE ID : CVE-2022-33925**	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	A-DEL-WYSE-170822/136
N/A	10-Aug-2022	6.5	Dell Wyse Management Suite 3.6.1 and below contains an improper access control vulnerability. A remote malicious	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-	A-DEL-WYSE-170822/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user could exploit this vulnerability in order to retain access to a file repository after it has been revoked. **CVE ID : CVE-2022-33926**	suite-security-update-for-multiple-vulnerabilities	
Session Fixation	10-Aug-2022	6.5	Dell Wyse Management Suite 3.6.1 and below contains a Session Fixation vulnerability. A unauthenticated attacker could exploit this by taking advantage of a user with multiple active sessions in order to hijack a user's session. **CVE ID : CVE-2022-33927**	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	A-DEL-WYSE-170822/138
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Aug-2022	6.5	WMS 3.7 contains a Path Traversal Vulnerability in Device API. An attacker could potentially exploit this vulnerability, to gain unauthorized read access to the files stored on the server filesystem, with the privileges of the running web application. **CVE ID : CVE-2022-34365**	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	A-DEL-WYSE-170822/139
Improper Neutralizat	10-Aug-2022	6.1	Dell Wyse Management Suite	https://www.dell.com/suppor	A-DEL-WYSE-170822/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			3.6.1 and below contains a Reflected Cross-Site Scripting Vulnerability in EndUserSummary page. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery. **CVE ID : CVE-2022-33929**	t/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	
N/A	10-Aug-2022	5.3	Dell Wyse Management Suite 3.6.1 and below contains an Improper Access control vulnerability with which an attacker with no access to create rules could potentially exploit this vulnerability and create rules. **CVE ID : CVE-2022-33924**	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	A-DEL-WYSE-170822/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Aug-2022	5.3	Dell Wyse Management Suite 3.6.1 and below contains an Improper Access control vulnerability in UI. An attacker with no access to Alert Classification page could potentially exploit this vulnerability, leading to the change the alert categories. **CVE ID : CVE-2022-33931**	https://www.dell.com/support/kbdoc/en-us/000201383/dsa-2022-134-dell-wyse-management-suite-security-update-for-multiple-vulnerabilities	A-DEL-WYSE-170822/142
Vendor: designwall					
Product: dw_promobar					
Affected Version(s): * Up to (including) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The DW Promobar WordPress plugin through 1.0.4 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 when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2423**	N/A	A-DES-DW_P-170822/143
Vendor: Devexpress					
Product: devexpress					
Affected Version(s): 22.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**	N/A	A-DEV-DEVE-170822/144
Affected Version(s): From (including) 18.1.0 Up to (excluding) 18.1.18					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack	N/A	A-DEV-DEVE-170822/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**		
Affected Version(s): From (including) 18.2.0 Up to (excluding) 18.2.17					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710.	N/A	A-DEV-DEVE-170822/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28684		
Affected Version(s): From (including) 19.1.0 Up to (excluding) 19.1.15					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**	N/A	A-DEV-DEVE-170822/147
Affected Version(s): From (including) 19.2.0 Up to (excluding) 19.2.14					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw	N/A	A-DEV-DEVE-170822/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**		
Affected Version(s): From (including) 20.1.0 Up to (excluding) 20.1.15					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service	N/A	A-DEV-DEVE-170822/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**		
Affected Version(s): From (including) 20.2.0 Up to (excluding) 20.2.11					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**	N/A	A-DEV-DEVE-170822/150
Affected Version(s): From (including) 21.1.0 Up to (excluding) 21.1.9					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit	N/A	A-DEV-DEVE-170822/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**		
Affected Version(s): From (including) 21.2.0 Up to (excluding) 21.2.7					
Deserialization of Untrusted Data	03-Aug-2022	8.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of DevExpress. Authentication is required to exploit this vulnerability. The specific flaw exists within the SafeBinaryFormatter library. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to	N/A	A-DEV-DEVE-170822/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute code in the context of the service account. Was ZDI-CAN-16710. **CVE ID : CVE-2022-28684**		
Vendor: digiprove					
Product: copyright_proof					
Affected Version(s): * Up to (including) 4.16					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	6.1	The Copyright Proof WordPress plugin through 4.16 does not sanitise and escape a parameter before outputting it back via an AJAX action available to both unauthenticated and authenticated users, leading to a Reflected Cross-Site Scripting when a specific setting is enabled. **CVE ID : CVE-2022-1906**	N/A	A-DIG-COPY-170822/153
Vendor: digital_product_labs					
Product: wpdating					
Affected Version(s): * Up to (including) 7.1.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	9.8	The WPDating WordPress plugin through 7.1.9 does not properly escape user input before concatenating it to certain SQL queries, leading to multiple SQL injection vulnerabilities.	N/A	A-DIG-WPDA-170822/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2460		
Vendor: discourse					
Product: discourse					
Affected Version(s): * Up to (excluding) 2.8.7					
Improper Resource Shutdown or Release	01-Aug-2022	5.3	Discourse is the an open source discussion platform. In affected versions a maliciously crafted request for static assets could cause error responses to be cached by Discourse's default NGINX proxy configuration. A corrected NGINX configuration is included in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-31182**	https://github.com/discourse/discourse/commit/7af25544c3940c4d046c51f4cfac9c72a06d4f50, https://github.com/discourse/discourse/security/advisories/GHSA-4ff8-3j78-w6pp	A-DIS-DISC-170822/155
Affected Version(s): * Up to (including) 2.8.6					
Allocation of Resources Without Limits or Throttling	01-Aug-2022	7.5	Discourse is the an open source discussion platform. In affected versions an email activation route can be abused to send mass spam emails. A fix has been included in the latest stable, beta and tests-passed	https://github.com/discourse/discourse/security/advisories/GHSA-m5w9-8gp8-2hrf, https://github.com/discourse/discourse/commit/af1cb735db7fb73217b8	A-DIS-DISC-170822/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of Discourse which rate limits emails. Users are advised to upgrade. Users unable to upgrade should manually rate limit email. **CVE ID : CVE-2022-31184**	5d22dbadd1bc824ac0b0	
Affected Version(s): 2.9.0					
Allocation of Resources Without Limits or Throttling	01-Aug-2022	7.5	Discourse is the an open source discussion platform. In affected versions an email activation route can be abused to send mass spam emails. A fix has been included in the latest stable, beta and tests-passed versions of Discourse which rate limits emails. Users are advised to upgrade. Users unable to upgrade should manually rate limit email. **CVE ID : CVE-2022-31184**	https://github.com/discourse/discourse/security/advisories/GHSA-m5w9-8gp8-2hrf, https://github.com/discourse/discourse/commit/af1cb735db7fb73217b85d22dbadd1bc824ac0b0	A-DIS-DISC-170822/157
Improper Resource Shutdown or Release	01-Aug-2022	5.3	Discourse is the an open source discussion platform. In affected versions a maliciously crafted request for static assets could cause error responses to be cached by Discourse's default	https://github.com/discourse/discourse/commit/7af25544c3940c4d046c51f4cfac9c72a06d4f50, https://github.com/discourse/discourse/sec	A-DIS-DISC-170822/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NGINX proxy configuration. A corrected NGINX configuration is included in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-31182**	urity/advisories/GHSA-4ff8-3j78-w6pp	
Vendor: Djangoproject					
Product: django					
Affected Version(s): From (including) 3.2 Up to (excluding) 3.2.15					
Download of Code Without Integrity Check	03-Aug-2022	8.8	An issue was discovered in the HTTP FileResponse class in Django 3.2 before 3.2.15 and 4.0 before 4.0.7. An application is vulnerable to a reflected file download (RFD) attack that sets the Content-Disposition header of a FileResponse when the filename is derived from user-supplied input. **CVE ID : CVE-2022-36359**	https://docs.djangoproject.com/en/4.0/releases/security/, https://www.djangoproject.com/weblog/2022/aug/03/security-releases/, http://www.openwall.com/lists/oss-security/2022/08/03/1	A-DJA-DJAN-170822/159
Affected Version(s): From (including) 4.0 Up to (excluding) 4.0.7					
Download of Code Without	03-Aug-2022	8.8	An issue was discovered in the HTTP FileResponse	https://docs.djangoproject.com/en/4.0/rele	A-DJA-DJAN-170822/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integrity Check			class in Django 3.2 before 3.2.15 and 4.0 before 4.0.7. An application is vulnerable to a reflected file download (RFD) attack that sets the Content-Disposition header of a FileResponse when the filename is derived from user-supplied input. **CVE ID : CVE-2022-36359**	ases/security/, https://www.djangoproject.com/weblog/2022/aug/03/security-releases/, http://www.openwall.com/lists/oss-security/2022/08/03/1	
Vendor: Dotcms					
Product: dotcms					
Affected Version(s): * Up to (including) 22.06					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	** DISPUTED ** A Reflected Cross-site scripting (XSS) issue was discovered in dotCMS Core through 22.06. This occurs in the admin portal when the configuration has XSS_PROTECTION_ENABLED=false. NOTE: the vendor disputes this because the current product behavior, in effect, has XSS_PROTECTION_ENABLED=true in all configurations. **CVE ID : CVE-2022-37431**	N/A	A-DOT-DOTC-170822/161
Vendor: duraspace					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: dspace					
Affected Version(s): From (excluding) 4.0 Up to (excluding) 6.4					
Generation of Error Message Containing Sensitive Information	01-Aug-2022	5.3	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. When an "Internal System Error" occurs in the JSPUI, then entire exception (including stack trace) is available. Information in this stacktrace may be useful to an attacker in launching a more sophisticated attack. This vulnerability only impacts the JSPUI. This issue has been fixed in version 6.4. users are advised to upgrade. Users unable to upgrade should disable the display of error messages in their internal.jsp file. **CVE ID : CVE-2022-31189**	https://github.com/DSpace/DSpace/security/advisories/GHSA-c2j7-66m3-r4ff, https://github.com/DSpace/DSpace/commit/afcc6c3389729b85d5c7b0230cbf9aaf7452f31a	A-DUR-DSPA-170822/162
Affected Version(s): From (excluding) 4.0 Up to (including) 5.10					
Improper Neutralization of Input During	01-Aug-2022	6.1	DSpace open source software is a repository application which provides durable	https://github.com/DSpace/DSpace/commit/c89e493e517b424dea6175ca	A-DUR-DSPA-170822/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI spellcheck "Did you mean" HTML escapes the data-spell attribute in the link, but not the actual displayed text. Similarly, the JSPUI autocomplete HTML does not properly escape text passed to it. Both are vulnerable to XSS. This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31191**	ba54e91d3847fc3a, https://github.com/DSpace/DSpace/commit/35030a23e48b5946f5853332c797e1c4adea7bb7, https://github.com/DSpace/DSpace/commit/ebb83a75234d3de9be129464013e998dc929b68d	
Affected Version(s): From (excluding) 6.0 Up to (excluding) 6.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Aug-2022	7.2	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI resumable upload implementations in SubmissionController and FileUploadRequest are vulnerable to	https://github.com/DSpace/DSpace/security/advisories/GHSA-qp5m-c3m9-8q2p, https://github.com/DSpace/DSpace/commit/7569c6374aefeafb996e202cf8d631020eda5f24, https://github.com/DSpace/DSpace/commit/	A-DUR-DSPA-170822/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			multiple path traversal attacks, allowing an attacker to create files/directories anywhere on the server writable by the Tomcat/DSpace user, by modifying some request parameters during submission. This path traversal can only be executed by a user with special privileges (submitter rights). This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds. However, this vulnerability cannot be exploited by an anonymous user or a basic user. The user must first have submitter privileges to at least one Collection and be able to determine how to modify the request parameters to exploit the vulnerability. **CVE ID : CVE-2022-31194**	d1dd7d23329ef055069759df15cfa200c8e3	
Improper Limitation of a Pathname	01-Aug-2022	7.2	DSpace open source software is a repository application which	https://github.com/DSpace/DSpace/commit/56e76049185b	A-DUR-DSPA-170822/165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			provides durable access to digital resources. In affected versions the ItemImportServiceImpl is vulnerable to a path traversal vulnerability. This means a malicious SAF (simple archive format) package could cause a file/directory to be created anywhere the Tomcat/DSpace user can write to on the server. However, this path traversal vulnerability is only possible by a user with special privileges (either Administrators or someone with command-line access to the server). This vulnerability impacts the XMLUI, JSPUI and command-line. Users are advised to upgrade. As a basic workaround, users may block all access to the following URL paths: If you are using the XMLUI, block all access to /admin/batchimport path (this is the URL of the Admin Batch Import tool). Keep in mind, if your site uses the path "/xmlui", then you'd	bd87c994128a9d77735ad7af0199, https://github.com/DSpace/DSpace/security/advisories/GHSA-8rmh-55h4-93h5, https://github.com/DSpace/DSpace/commit/7af52a0883a9dbc475cf3001f04ed11b24c8a4c0	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			need to block access to /xmlui/admin/batch import. If you are using the JSPUI, block all access to /dspace-admin/batchimport path (this is the URL of the Admin Batch Import tool). Keep in mind, if your site uses the path "/jspui", then you'd need to block access to /jspui/dspace-admin/batchimport. Keep in mind, only an Administrative user or a user with command-line access to the server is able to import/upload SAF packages. Therefore, assuming those users do not blindly upload untrusted SAF packages, then it is unlikely your site could be impacted by this vulnerability. **CVE ID : CVE-2022-31195**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	6.1	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for	https://github.com/DSpace/DSpace/commit/c89e493e517b424dea6175caba54e91d3847fc3a, https://github.com/DSpace/D	A-DUR-DSPA-170822/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DSpace. The JSPUI spellcheck "Did you mean" HTML escapes the data-spell attribute in the link, but not the actual displayed text. Similarly, the JSPUI autocomplete HTML does not properly escape text passed to it. Both are vulnerable to XSS. This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31191**	Space/commit/35030a23e48b5946f5853332c797e1c4adea7bb7, https://github.com/DSpace/DSpace/commit/ebb83a75234d3de9be129464013e998dc929b68d	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	6.1	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI "Request a Copy" feature does not properly escape values submitted and stored from the "Request a Copy" form. This means that item requests could be vulnerable to XSS attacks. This vulnerability only	https://github.com/DSpace/DSpace/commit/f7758457b7ec3489d525e39aa753cc70809d9ad9, https://github.com/DSpace/DSpace/security/advisories/GHSA-4wm8-c2vv-xrpq, https://github.com/DSpace/DSpace/commit/28eb8158210d41168a62ed5f9e044f754513bc37	A-DUR-DSPA-170822/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts the JSPUI. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-31192**		
URL Redirection to Untrusted Site ('Open Redirect')	01-Aug-2022	6.1	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI controlled vocabulary servlet is vulnerable to an open redirect attack, where an attacker can craft a malicious URL that looks like a legitimate DSpace/repository URL. When that URL is clicked by the target, it redirects them to a site of the attacker's choice. This issue has been patched in versions 5.11 and 6.4. Users are advised to upgrade. There are no known workaround for this vulnerability. **CVE ID : CVE-2022-31193**	https://github.com/DSpace/DSpace/commit/f7758457b7ec3489d525e39aa753cc70809d9ad9, https://github.com/DSpace/DSpace/commit/5f72424a478f59061dcc516b866dcc687bc3f9de, https://github.com/DSpace/DSpace/security/advisories/GHSA-763j-q7wv-vf3m	A-DUR-DSPA-170822/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.0 Up to (excluding) 6.4					
Exposure of Sensitive Information to an Unauthorized Actor	01-Aug-2022	5.3	DSpace open source software is a repository application which provides durable access to digital resources. dspace-xmlui is a UI component for DSpace. In affected versions metadata on a withdrawn Item is exposed via the XMLUI "mets.xml" object, as long as you know the handle/URL of the withdrawn Item. This vulnerability only impacts the XMLUI. Users are advised to upgrade to version 6.4 or newer. **CVE ID : CVE-2022-31190**	https://github.com/DSpace/DSpace/security/advisories/GHSA-7w85-pp86-p4pq, https://github.com/DSpace/DSpace/pull/2451, https://github.com/DSpace/DSpace/commit/574e25496a40173653ae7d0a49a19ed8e3458606.patch	A-DUR-DSPA-170822/169
Affected Version(s): From (including) 4.0 Up to (including) 5.10					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Aug-2022	7.2	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI resumable upload implementations in SubmissionController and FileUploadRequest	https://github.com/DSpace/DSpace/security/advisories/GHSA-qp5m-c3m9-8q2p, https://github.com/DSpace/DSpace/commit/7569c6374aefeafb996e202cf8d631020eda5f24, https://github.com/DSpace/D	A-DUR-DSPA-170822/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are vulnerable to multiple path traversal attacks, allowing an attacker to create files/directories anywhere on the server writable by the Tomcat/DSpace user, by modifying some request parameters during submission. This path traversal can only be executed by a user with special privileges (submitter rights). This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds. However, this vulnerability cannot be exploited by an anonymous user or a basic user. The user must first have submitter privileges to at least one Collection and be able to determine how to modify the request parameters to exploit the vulnerability. **CVE ID : CVE-2022-31194**	Space/commit/d1dd7d23329ef055069759df15cfa200c8e3	
Improper Limitation of a	01-Aug-2022	7.2	DSpace open source software is a repository	https://github.com/DSpace/DSpace/commit/	A-DUR-DSPA-170822/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			application which provides durable access to digital resources. In affected versions the ItemImportServiceImpl is vulnerable to a path traversal vulnerability. This means a malicious SAF (simple archive format) package could cause a file/directory to be created anywhere the Tomcat/DSpace user can write to on the server. However, this path traversal vulnerability is only possible by a user with special privileges (either Administrators or someone with command-line access to the server). This vulnerability impacts the XMLUI, JSPUI and command-line. Users are advised to upgrade. As a basic workaround, users may block all access to the following URL paths: If you are using the XMLUI, block all access to /admin/batchimport path (this is the URL of the Admin Batch Import tool). Keep in mind, if your site uses the path	56e76049185bbd87c994128a9d77735ad7af0199, https://github.com/DSpace/DSpace/security/advisories/GHSA-8rmh-55h4-93h5, https://github.com/DSpace/DSpace/commit/7af52a0883a9dbc475cf3001f04ed11b24c8a4c0	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			"/xmlui", then you'd need to block access to /xmlui/admin/batchimport. If you are using the JSPUI, block all access to /dspace-admin/batchimport path (this is the URL of the Admin Batch Import tool). Keep in mind, if your site uses the path "/jspui", then you'd need to block access to /jspui/dspace-admin/batchimport. Keep in mind, only an Administrative user or a user with command-line access to the server is able to import/upload SAF packages. Therefore, assuming those users do not blindly upload untrusted SAF packages, then it is unlikely your site could be impacted by this vulnerability. **CVE ID : CVE-2022-31195**		
Improper Neutralization of Input During Web Page Generation	01-Aug-2022	6.1	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI	https://github.com/DSpace/DSpace/commit/f7758457b7ec3489d525e39aa753cc70809d9ad9, https://github.	A-DUR-DSPA-170822/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			component for DSpace. The JSPUI "Request a Copy" feature does not properly escape values submitted and stored from the "Request a Copy" form. This means that item requests could be vulnerable to XSS attacks. This vulnerability only impacts the JSPUI. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2022-31192**	com/DSpace/DSpace/security/advisories/GHSA-4wm8-c2vv-xrpq, https://github.com/DSpace/DSpace/commit/28eb8158210d41168a62ed5f9e044f754513bc37	
URL Redirection to Untrusted Site ('Open Redirect')	01-Aug-2022	6.1	DSpace open source software is a repository application which provides durable access to digital resources. dspace-jspui is a UI component for DSpace. The JSPUI controlled vocabulary servlet is vulnerable to an open redirect attack, where an attacker can craft a malicious URL that looks like a legitimate DSpace/repository URL. When that URL is clicked by the target, it redirects	https://github.com/DSpace/DSpace/commit/f7758457b7ec3489d525e39aa753cc70809d9ad9, https://github.com/DSpace/DSpace/commit/5f72424a478f59061dcc516b866dcc687bc3f9de, https://github.com/DSpace/DSpace/security/advisories/GHSA-763j-q7wv-vf3m	A-DUR-DSPA-170822/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			them to a site of the attacker's choice. This issue has been patched in versions 5.11 and 6.4. Users are advised to upgrade. There are no known workaround for this vulnerability. **CVE ID : CVE-2022-31193**		
Vendor: easyuse					
Product: mailhunter_ultimate					
Affected Version(s): * Up to (including) 2020					
Deserialization of Untrusted Data	02-Aug-2022	9.8	EasyUse MailHunter Ultimate's cookie deserialization function has an inadequate validation vulnerability. Deserializing a cookie containing malicious payload will trigger this insecure deserialization vulnerability, allowing an unauthenticated remote attacker to execute arbitrary code, manipulate system command or interrupt service. **CVE ID : CVE-2022-35223**	N/A	A-EAS-MAIL-170822/174
Vendor: easy_username_updater_project					
Product: easy_username_updater					
Affected Version(s): * Up to (excluding) 1.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	08-Aug-2022	6.5	The Easy Username Updater WordPress plugin before 1.0.5 does not implement CSRF checks, which could allow attackers to make a logged in admin change any user's username includes the admin **CVE ID : CVE-2022-2355**	N/A	A-EAS-EASY-170822/175
Vendor: elabftw					
Product: elabftw					
Affected Version(s): * Up to (excluding) 4.3.4					
Incorrect Authorization	01-Aug-2022	4.3	eLabFTW is an electronic lab notebook manager for research teams. A vulnerability was discovered which allows a logged in user to read a template without being authorized to do so. This vulnerability has been patched in 4.3.4. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31178**	https://github.com/elabftw/elabftw/security/advisories/GHSA-63qq-hw97-8q7x	A-ELA-ELAB-170822/176
Vendor: electronic_medical_records_system_project					
Product: electronic_medical_records_system					
Affected Version(s): -					
Improper Neutralization of	05-Aug-2022	9.8	A vulnerability was found in SourceCodester	N/A	A-ELE-ELEC-170822/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Electronic Medical Records System and classified as critical. Affected by this issue is some unknown functionality of the component POST Request Handler. The manipulation of the argument user_email 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-205664. **CVE ID : CVE-2022-2676**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2022	8.8	A vulnerability has been found in SourceCodester Electronic Medical Records System and classified as critical. This vulnerability affects unknown code of the file register.php of the component UPDATE Statement Handler. The manipulation of the argument pconsultation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be	N/A	A-ELE-ELEC-170822/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The identifier of this vulnerability is VDB-205816. **CVE ID : CVE-2022-2693**		
Vendor: employee_management_system_project					
Product: employee_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2022	9.8	A vulnerability has been found in SourceCodester Employee Management System and classified as critical. This vulnerability affects unknown code of the file eloginwel.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-205834 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2715**	N/A	A-EMP-EMPL-170822/179
Improper Neutralization of Special Elements used in an SQL Command	09-Aug-2022	9.8	A vulnerability was found in SourceCodester Employee Management System. It has been classified as critical. Affected is an unknown function of the file /process/eprocess.p	N/A	A-EMP-EMPL-170822/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			hp. The manipulation of the argument mailuid/pwd 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-205836. **CVE ID : CVE-2022-2723**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2022	9.8	A vulnerability was found in SourceCodester Employee Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /process/aprocess.php. The manipulation of the argument mailuid 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-205837 was assigned to this vulnerability. **CVE ID : CVE-2022-2724**	N/A	A-EMP-EMPL-170822/181
Vendor: Enalean					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: tuleap					
Affected Version(s): From (including) 13.10 Up to (excluding) 13.10-3					
Missing Authorization	01-Aug-2022	5.4	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions Tuleap does not properly verify permissions when creating branches with the REST API in Git repositories using the fine grained permissions. Users can create branches via the REST endpoint `POST git/:id/branches` regardless of the permissions set on the repository. This issue has been fixed in version 13.10.99.82 Tuleap Community Edition as well as in version 13.10-3 of Tuleap Enterprise Edition. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31128**	https://github.com/Enalean/tuleap/security/advisories/GHSA-2p49-vgcx-5w79, https://github.com/Enalean/tuleap/commit/58ecb1dee1c46075d3e089980301ebfbe0bafd33, https://tuleap.net/plugins/tracker/?aid=27538	A-ENA-TULE-170822/182
Affected Version(s): From (including) 13.9.9.110 Up to (excluding) 13.10.99.82					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	01-Aug-2022	5.4	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In affected versions Tuleap does not properly verify permissions when creating branches with the REST API in Git repositories using the fine grained permissions. Users can create branches via the REST endpoint `POST git/:id/branches` regardless of the permissions set on the repository. This issue has been fixed in version 13.10.99.82 Tuleap Community Edition as well as in version 13.10-3 of Tuleap Enterprise Edition. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31128**	https://github.com/Enalean/tuleap/security/advisories/GHSA-2p49-vgcx-5w79, https://github.com/Enalean/tuleap/commit/58ecb1dee1c46075d3e089980301ebfbe0bafd33, https://tuleap.net/plugins/tracker/?aid=27538	A-ENA-TULE-170822/183
Vendor: Estsoft					
Product: alyac					
Affected Version(s): 2.5.8.544					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow to Buffer Overflow	05-Aug-2022	7.8	An integer overflow vulnerability exists in the way ESTsoft Alyac 2.5.8.544 parses OLE files. A specially-crafted OLE file can lead to a heap buffer overflow, which can result in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-29886**	N/A	A-EST-ALYA-170822/184
Integer Overflow to Buffer Overflow	05-Aug-2022	7.8	An integer overflow vulnerability exists in the way ESTsoft Alyac 2.5.8.544 parses OLE files. A specially-crafted OLE file can lead to a heap buffer overflow which can result in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-32543**	N/A	A-EST-ALYA-170822/185
Vendor: ethereum					
Product: go_ethereum					
Affected Version(s): * Up to (including) 1.10.21					
N/A	05-Aug-2022	5.9	Go Ethereum (aka geth) through 1.10.21 allows attackers to increase rewards by mining	N/A	A-ETH-GO_E-170822/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			blocks in certain situations, and using a manipulation of time-difference values to achieve replacement of main-chain blocks, aka Riskless Uncle Making (RUM), as exploited in the wild in 2020 through 2022. **CVE ID : CVE-2022-37450**		
Vendor: evmos					
Product: ethermint					
Affected Version(s): * Up to (excluding) 0.18.0					
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.3	Ethermint is an Ethereum library. In Ethermint running versions before `v0.17.2`, the contract `selfdestruct` invocation permanently removes the corresponding bytecode from the internal database storage. However, due to a bug in the `DeleteAccount`function, all contracts that used the identical bytecode (i.e shared the same `CodeHash`) will also stop working once one contract invokes `selfdestruct`, even though the other	https://github.com/evmos/ethermint/commit/144741832007a26dbe950512acbda4ed95b2a451, https://github.com/evmos/ethermint/security/advisories/GHSA-f92v-grc2-w2fg	A-EVM-ETHE-170822/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contracts did not invoke the `selfdestruct` OPCODE. This vulnerability has been patched in Ethermint version v0.18.0. The patch has state machine-breaking changes for applications using Ethermint, so a coordinated upgrade procedure is required. A workaround is available. If a contract is subject to DoS due to this issue, the user can redeploy the same contract, i.e. with identical bytecode, so that the original contract's code is recovered. The new contract deployment restores the `bytecode hash -> bytecode` entry in the internal state. **CVE ID : CVE-2022-35936**		
Product: evmos					
Affected Version(s): * Up to (excluding) 7.0.0					
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.3	Ethermint is an Ethereum library. In Ethermint running versions before `v0.17.2`, the contract `selfdestruct` invocation	https://github.com/evmos/ethermint/commit/144741832007a26dbe950512acbda4ed95b2a451, https://github.	A-EVM-EVMO-170822/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permanently removes the corresponding bytecode from the internal database storage. However, due to a bug in the `DeleteAccount`function, all contracts that used the identical bytecode (i.e shared the same `CodeHash`) will also stop working once one contract invokes `selfdestruct`, even though the other contracts did not invoke the `selfdestruct` OPCODE. This vulnerability has been patched in Ethermint version v0.18.0. The patch has state machine-breaking changes for applications using Ethermint, so a coordinated upgrade procedure is required. A workaround is available. If a contract is subject to DoS due to this issue, the user can redeploy the same contract, i.e. with identical bytecode, so that the original contract's code is recovered. The new contract deployment	com/evmos/ethermint/security/advisories/GHSA-f92v-grc2-w2fg	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restores the `bytecode hash -> bytecode` entry in the internal state. **CVE ID : CVE-2022-35936**		
Vendor: Exim					
Product: exim					
Affected Version(s): * Up to (excluding) 4.95					
Out-of-bounds Write	07-Aug-2022	9.8	Exim before 4.95 has a heap-based buffer overflow for the alias list in host_name_lookup in host.c when sender_host_name is set. **CVE ID : CVE-2022-37452**	https://www.exim.org/static/doc/security/, https://github.com/ivd38/exim_overflow, https://github.com/Exim/exim/commit/d4bc023436e4cce7c23c5f8bb5199e178b4cc743, https://github.com/Exim/exim/compare/exim-4.94...exim-4.95	A-EXI-EXIM-170822/189
Affected Version(s): * Up to (excluding) 4.96					
Release of Invalid Pointer or Reference	06-Aug-2022	7.5	Exim before 4.96 has an invalid free in pam_converse in auths/call_pam.c because store_free is not used after store_malloc. **CVE ID : CVE-2022-37451**	https://www.exim.org/static/doc/security/, https://github.com/ivd38/exim_invalid_free, https://lists.exim.org/lurker/message/20220625.141825.d6de6074.en.html, https://github.com/Exim/exim/commit/51b	A-EXI-EXIM-170822/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				e321b27825c01829dffd90f11bfff256f7e42	
Vendor: expense_management_system_project					
Product: expense_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2022	9.8	A vulnerability was found in SourceCodester Expense Management System. It has been rated as critical. This issue affects the function fetch_report_credit of the file report.php of the component POST Parameter Handler. The manipulation of the argument from/to leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-205811. **CVE ID : CVE-2022-2688**	N/A	A-EXP-EXPE-170822/191
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): 1.5.8					
Improper Neutralization of Input During Web Page Generation	10-Aug-2022	5.4	An issue was discovered in EyouCMS 1.5.8. There is a Storage XSS vulnerability that can allows an attacker to execute arbitrary Web	N/A	A-EYO-EYOU-170822/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			scripts or HTML by injecting a special payload via the title parameter in the foreground contribution, allowing the attacker to obtain sensitive information. **CVE ID : CVE-2022-35509**		
Vendor: F-secure					
Product: atlant					
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	A-F-S-ATLA-170822/193
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/sec	A-F-S-ATLA-170822/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	urity-advisories	
Product: cloud_protection_for_salesforce					
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	A-F-S-CLOU-170822/195
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-CLOU-170822/196
Product: elements_collaboration_protection					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	A-F-S-ELEM-170822/197
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-ELEM-170822/198
Product: elements_endpoint_detection_and_response					
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-	A-F-S-ELEM-170822/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	of-fame, https://www.withsecure.com/en/expertise/people	
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-ELEM-170822/200
Product: elements_endpoint_protection					
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	A-F-S-ELEM-170822/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely by an attacker. **CVE ID : CVE-2022-28880**		
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-ELEM-170822/202
Product: internet_gatekeeper					
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	A-F-S-INTE-170822/203
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability	https://www.f-secure.com/en	A-F-S-INTE-170822/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	
Product: linux_security					
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	A-F-S-LINU-170822/205
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/	A-F-S-LINU-170822/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which leads to scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	en/support/security-advisories	
Product: linux_security_64					
Affected Version(s): *					
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	A-F-S-LINU-170822/207
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker.	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	A-F-S-LINU-170822/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28881		
Vendor: F5					
Product: big-ip_access_policy_manager					
Affected Version(s): 16.1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.7	In BIG-IP Versions 16.1.x before 16.1.1 and 15.1.x before 15.1.4, when running in Appliance mode, an authenticated attacker may be able to bypass Appliance mode restrictions due to a directory traversal vulnerability in an undisclosed page within iApps. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-31473**	https://support.f5.com/csp/article/K34893234	A-F5-BIG--170822/209
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/211
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	ticle/K50310001	
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35272		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/214
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/216
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/218
Loop with Unreachable Exit	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	ticle/K66510514	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/221
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/223
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/226
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when a BIG-IP APM access policy with Service Connect agent is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K52534925	A-F5-BIG--170822/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33203**		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/228
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM)	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/230
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/232
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5.1, when a BIG-IP APM access policy	https://support.f5.com/csp/article/K58235223	A-F5-BIG--170822/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35245**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/235
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/237
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.7	In BIG-IP Versions 16.1.x before 16.1.1 and 15.1.x before 15.1.4, when running in Appliance mode, an authenticated attacker may be able to bypass Appliance mode restrictions due to a directory traversal	https://support.f5.com/csp/article/K34893234	A-F5-BIG--170822/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in an undisclosed page within iApps. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-31473**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/240
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/242
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when a BIG-IP APM access policy with Service Connect agent is configured on a virtual server, undisclosed requests can cause an	https://support.f5.com/csp/article/K52534925	A-F5-BIG--170822/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33203**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/244
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/247
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/249
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5.1, when a BIG-IP APM access policy is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K58235223	A-F5-BIG--170822/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35245		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/251
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address,	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/253
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x,	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/255
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/256
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/258
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when a BIG-IP APM access policy with Service Connect agent is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33203**	https://support.f5.com/csp/article/K52534925	A-F5-BIG--170822/260
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	ticle/K55580033	
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34651		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/263
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization,	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5.1, when a BIG-IP APM access policy is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35245**	https://support.f5.com/csp/article/K58235223	A-F5-BIG--170822/265
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/268
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/270
Product: big-ip_advanced_firewall_manager					
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/272
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	ticle/K50310001	
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35272		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/275
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/277
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/279
Loop with Unreachable Exit	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	ticle/K66510514	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/282
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/284
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/287
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/289
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/291
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/294
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/296
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/298
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32455		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/301
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/303
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/305
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/308
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/310
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server,	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/312
Uncontrolled Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	ticle/K79933541	
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/314
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/315
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/317
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34862		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/320
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address,	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/322
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/324
Product: big-ip_analytics					
Affected Version(s): 17.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/325
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/327
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/329
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/331
Improper Privilege	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	ticle/K11010341	
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM)	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/334
Improper Neutralization of Special Elements in Output Used by a Downstream Component	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/336
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	ticle/K50310001	
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33968		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/339
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary.	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/341
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/343
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/345
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	ticle/K55580033	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/348
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/350
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/352
Improper Privilege	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	ticle/K11010341	
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM)	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/355
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/358
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/360
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation.	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/362
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/364
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	ticle/K93504311	
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/367
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/369
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/372
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/374
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/377
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Product: big-ip_application_acceleration_manager					
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/379
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/381
Improper Resource	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	ticle/K90024104	
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33968		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/384
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/386
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/388
Improper Neutralization of Special	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	ticle/K13213418	
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/391
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use,	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/393
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/396
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/398
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/400
Improper Neutralization of Special Elements in Output Used by a Downstream Component	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/403
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/405
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/407
Improper Restriction of Operations within the	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5,	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34651		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/410
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate.	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/412
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server,	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/414
Improper Neutralization of Special Elements in Output Used by a	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33962		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/417
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/419
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/421
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/424
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond,	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/427
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/429
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/431
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Product: big-ip_application_security_manager					
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/434
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/436
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/439
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/441
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/443
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34851		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/446
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/448
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/450
Loop with Unreachable Exit Condition	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	ticle/K66510514	
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/452
Improper Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and	https://support.f5.com/csp/ar	A-F5-BIG--170822/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	ticle/K28405643	
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/455
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/457
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35728		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/460
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/462
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/464
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/467
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/469
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/471
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34655		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/474
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/476
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35728		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/479
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate.	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/481
Improper Neutralization of Special Elements in Output Used by a Downstrea	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/484
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/486
Product: big-ip_domain_name_system					
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/488
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	ticle/K50310001	
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35272		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/491
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/493
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/495
Loop with Unreachable Exit	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	ticle/K66510514	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/498
Deserialization of Untrusted Data	04-Aug-2022	6.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, a vulnerability exists in undisclosed pages of the BIG-IP DNS Traffic Management User Interface (TMUI) that allows an authenticated attacker with at least operator role	https://support.f5.com/csp/article/K38893457	A-F5-BIG--170822/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges to cause the Tomcat process to restart and perform unauthorized DNS requests and operations through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33947**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/501
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34865		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/503
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/505
Loop with Unreachable Exit Condition	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/507
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Deserialization of Untrusted Data	04-Aug-2022	6.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, a vulnerability exists in undisclosed pages of the BIG-IP DNS Traffic Management User Interface (TMUI) that allows an authenticated attacker with at least operator role privileges to cause the Tomcat process to restart and perform unauthorized DNS requests and operations through undisclosed requests. Note: Software versions	https://support.f5.com/csp/article/K38893457	A-F5-BIG--170822/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33947**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/510
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Manageme nt	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://suppor t.f5.com/csp/ar ticle/K809706 53	A-F5-BIG-- 170822/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/513
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/515
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/517
Improper Restriction of Operations within the	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5,	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34651		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/520
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate.	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/522
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server,	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/524
Improper Neutralization of Special Elements in Output Used by a	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33962		
Deserialization of Untrusted Data	04-Aug-2022	6.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, a vulnerability exists in undisclosed pages of the BIG-IP DNS Traffic Management User Interface (TMUI) that allows an authenticated attacker with at least operator role privileges to cause the Tomcat process to restart and perform unauthorized DNS requests and operations through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33947**	https://support.f5.com/csp/article/K38893457	A-F5-BIG--170822/527
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/529
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/530
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note:	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/532
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization.	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/534
Deserialization of Untrusted Data	04-Aug-2022	6.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K38893457	A-F5-BIG--170822/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5, and all versions of 13.1.x, a vulnerability exists in undisclosed pages of the BIG-IP DNS Traffic Management User Interface (TMUI) that allows an authenticated attacker with at least operator role privileges to cause the Tomcat process to restart and perform unauthorized DNS requests and operations through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33947**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/537
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/540
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/542
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server,	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/544
Product: big-ip_fraud_protection_service					
Affected Version(s): 17.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/545
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/547
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/549
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/551
Improper Privilege	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	ticle/K11010341	
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM)	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/554
Improper Neutralization of Special Elements in Output Used by a Downstream Component	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/556
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	ticle/K50310001	
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33968		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/559
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary.	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/561
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/563
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/565
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	ticle/K55580033	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/568
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/570
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/572
Improper Privilege	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	ticle/K11010341	
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM)	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/575
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/578
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/580
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation.	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/582
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/584
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	ticle/K93504311	
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/587
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/589
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/592
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/594
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/597
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Product: big-ip_global_traffic_manager					
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/599
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/601
Improper Resource	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	ticle/K90024104	
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33968		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/604
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/606
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/608
Improper Neutralization of Special	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	ticle/K13213418	
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/611
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use,	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/613
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/616
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/618
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/620
Improper Neutralization of Special Elements in Output Used by a Downstream Component	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/623
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/625
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/627
Improper Restriction of Operations within the	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5,	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34651		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/630
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate.	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/632
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server,	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/634
Improper Neutralization of Special Elements in Output Used by a	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33962		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/637
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/639
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/641
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/644
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond,	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/647
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/649
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/651
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Product: big-ip_link_controller					
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/654
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/656
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/659
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/661
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/663
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34851		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/666
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/668
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/670
Loop with Unreachable Exit Condition	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	ticle/K66510514	
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/672
Improper Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and	https://support.f5.com/csp/ar	A-F5-BIG--170822/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	ticle/K28405643	
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/675
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/677
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35728		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/680
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/682
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**		
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/684
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/687
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/689
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/691
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34655		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/694
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/696
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35728		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/699
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate.	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/701
Improper Neutralization of Special Elements in Output Used by a Downstrea	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/704
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/706
Product: big-ip_local_traffic_manager					
Affected Version(s): 17.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/708
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	ticle/K50310001	
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35272		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/711
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/713
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/715
Loop with Unreachable Exit	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	ticle/K66510514	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/718
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/720
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**		
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/723
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/725
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/727
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/730
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/732
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/734
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32455		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/737
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/739
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/741
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/744
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/746
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server,	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/748
Uncontrolled Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	ticle/K79933541	
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/750
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/751
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/753
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34862		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/756
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address,	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/758
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/760
Product: big-ip_policy_enforcement_manager					
Affected Version(s): 17.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/761
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/763
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/765
Affected Version(s): From (including) 13.1.0 Up to (including) 13.1.5					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/767
Improper Privilege	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	ticle/K11010341	
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM)	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/770
Improper Neutralization of Special Elements in Output Used by a Downstream Component	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/772
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1,	https://support.f5.com/csp/ar	A-F5-BIG--170822/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	ticle/K50310001	
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33968		
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/775
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary.	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/777
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/779
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**		
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/781
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	ticle/K55580033	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/784
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/786
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
Improper Certificate Validation	04-Aug-2022	9.1	In BIG-IP Versions 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, Traffic Intelligence feeds, which use HTTPS, do not verify the remote endpoint identity, allowing for potential data poisoning. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34865**	https://support.f5.com/csp/article/K25046752	A-F5-BIG--170822/788
Improper Privilege	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	ticle/K11010341	
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM)	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/791
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic	https://support.f5.com/csp/article/K93504311	A-F5-BIG--170822/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/794
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/796
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation.	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**		
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/798
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/800
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.1.1					
Use of Uninitialized Resource	04-Aug-2022	7.5	In BIG-IP Versions 16.0.x before 16.0.1.1, 15.1.x	https://support.f5.com/csp/ar	A-F5-BIG--170822/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 15.1.6.1, and 14.1.x before 14.1.5, when an iRule containing the HTTP::payload command is configured on a virtual server, undisclosed traffic can cause Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34655**	ticle/K93504311	
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2.2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when a BIG-IP LTM Client SSL profile is configured on a virtual server to perform client certificate authentication with session tickets enabled, undisclosed requests cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical	https://support.f5.com/csp/article/K16852653	A-F5-BIG--170822/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Support (EoTS) are not evaluated. **CVE ID : CVE-2022-32455**		
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when an HTTP2 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35236**	https://support.f5.com/csp/article/K79933541	A-F5-BIG--170822/803
Improper Resource Shutdown or Release	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.2.2, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when the Message Routing (MR) Message Queuing Telemetry Transport (MQTT) profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of	https://support.f5.com/csp/article/K28405643	A-F5-BIG--170822/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35240**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Improper Privilege Management	04-Aug-2022	9.1	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.5.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, using an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35243**	https://support.f5.com/csp/article/K11010341	A-F5-BIG--170822/805
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3.1					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
NULL Pointer Dereference	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, when an LTM Client or Server SSL profile with TLS 1.3 enabled is configured on a virtual server, along with an iRule that calls HTTP::respond, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34651**	https://support.f5.com/csp/article/K59197053	A-F5-BIG--170822/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/808
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when an LTM virtual server is configured to perform normalization, undisclosed requests can cause the Traffic	https://support.f5.com/csp/article/K66510514	A-F5-BIG--170822/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34862**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Aug-2022	7.2	In BIG-IP Versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, an authenticated attacker with Resource Administrator or Manager privileges can create or modify existing monitor objects in the Configuration utility in an undisclosed manner leading to a privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35735**	https://support.f5.com/csp/article/K13213418	A-F5-BIG--170822/810
Improper Privilege Management	04-Aug-2022	6.7	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x	https://support.f5.com/csp/article/K80970653	A-F5-BIG--170822/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 14.1.5.1, and all versions of 13.1.x, certain iRules commands may allow an attacker to bypass the access control restrictions for a self IP address, regardless of the port lockdown settings. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33962**		
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	04-Aug-2022	5.5	In BIG-IP Versions 17.0.x before 17.0.0.1 and 16.1.x before 16.1.3.1, when source-port preserve-strict is configured on an HTTP Message Routing Framework (MRF) virtual server, undisclosed traffic may cause the Traffic Management Microkernel (TMM) to produce a core file and the connection to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35272**	https://support.f5.com/csp/article/K90024104	A-F5-BIG--170822/813
Out-of-bounds Read	04-Aug-2022	4.9	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, when an LTM monitor or APM SSO is configured on a virtual server, and NTLM challenge-response is in use, undisclosed traffic can cause a buffer over-read. Note: Software versions which have reached	https://support.f5.com/csp/article/K23465404	A-F5-BIG--170822/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33968**		
Product: big-ip_ssl_orchestrator					
Affected Version(s): From (including) 14.1.0 Up to (excluding) 14.1.5					
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when a BIG-IP APM access policy with Service Connect agent is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33203**	https://support.f5.com/csp/article/K52534925	A-F5-BIG--170822/815
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.6.1					
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when a BIG-IP APM access policy with Service Connect agent is configured on a virtual server, undisclosed requests can cause an	https://support.f5.com/csp/article/K52534925	A-F5-BIG--170822/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33203**		
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.3					
Uncontrolled Resource Consumption	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, and 14.1.x before 14.1.5, when a BIG-IP APM access policy with Service Connect agent is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-33203**	https://support.f5.com/csp/article/K52534925	A-F5-BIG--170822/817
Product: big-iq_centralized_management					
Affected Version(s): 7.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Affected Version(s): 7.1.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/820
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**		
Affected Version(s): 8.0.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35728		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/823
Affected Version(s): 8.1.0					
Insufficient Session Expiration	04-Aug-2022	9.8	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ version 8.x before 8.2.0 and	https://support.f5.com/csp/article/K55580033	A-F5-BIG--170822/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			all versions of 7.x, an authenticated user's iControl REST token may remain valid for a limited time after logging out from the Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35728**		
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34844		
Affected Version(s): 8.2.0					
N/A	04-Aug-2022	7.5	In BIG-IP Versions 16.1.x before 16.1.3.1 and 15.1.x before 15.1.6.1, and all versions of BIG-IQ 8.x, when the Data Plane Development Kit (DPDK)/Elastic Network Adapter (ENA) driver is used with BIG-IP or BIG-IQ on Amazon Web Services (AWS) systems, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Successful exploitation relies on conditions outside of the attacker's control. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34844**	https://support.f5.com/csp/article/K34511555	A-F5-BIG--170822/826
Affected Version(s): From (including) 8.0.0 Up to (including) 8.2.0					
Improper Input Validation	04-Aug-2022	6.5	In BIG-IP Versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and all versions of 13.1.x,	https://support.f5.com/csp/article/K50310001	A-F5-BIG--170822/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and BIG-IQ Centralized Management all versions of 8.x, an authenticated attacker may cause iControl SOAP to become unavailable through undisclosed requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-34851**		
Product: nginx_ingress_controller					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 2.3.0					
Improper Input Validation	04-Aug-2022	6.5	In versions 2.x before 2.3.0 and all versions of 1.x, An attacker authorized to create or update ingress objects can obtain the secrets available to the NGINX Ingress Controller. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-30535**	https://support.f5.com/csp/article/K52125139	A-F5-NGIN-170822/828
Product: nginx_instance_manager					
Affected Version(s): From (including) 1.0.0 Up to (including) 1.0.4					
Uncontrolled Resource	04-Aug-2022	6.5	In versions 2.x before 2.3.1 and all versions of 1.x, when	https://support.f5.com/csp/ar	A-F5-NGIN-170822/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Consumption			NGINX Instance Manager is in use, undisclosed requests can cause an increase in disk resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35241**	ticle/K37080719	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.3.1					
Uncontrolled Resource Consumption	04-Aug-2022	6.5	In versions 2.x before 2.3.1 and all versions of 1.x, when NGINX Instance Manager is in use, undisclosed requests can cause an increase in disk resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID : CVE-2022-35241**	https://support.f5.com/csp/article/K37080719	A-F5-NGIN-170822/830
Vendor: fast_food_ordering_system_project					
Product: fast_food_ordering_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page	06-Aug-2022	5.4	A vulnerability, which was classified as problematic, was found in oretnom23 Fast Food Ordering System. This affects	N/A	A-FAS-FAST-170822/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			an unknown part of the component Menu List Page. The manipulation of the argument Description 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 identifier VDB-205725 was assigned to this vulnerability. **CVE ID : CVE-2022-2686**		
Vendor: fava_project					
Product: fava					
Affected Version(s): * Up to (excluding) 1.22.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository beancount/fava prior to 1.22.3. **CVE ID : CVE-2022-2589**	https://huntr.dev/bounties/8705800d-cf2f-433d-9c3e-dbef6a3f7e08, https://github.com/beancount/fava/commit/68bbb6e39319deb35ab9f18d0b6aa9fa70472539	A-FAV-FAVA-170822/832
Vendor: fifu					
Product: featured_image_from_url					
Affected Version(s): * Up to (excluding) 4.0.0					
Cross-Site Request Forgery (CSRF)	01-Aug-2022	6.1	The Featured Image from URL (FIFU) WordPress plugin before 4.0.0 does not have CSRF check in	N/A	A-FIF-FEAT-170822/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack. Furthermore, due to the lack of validation, sanitisation and escaping in some of them, it could also lead to Stored XSS issues **CVE ID : CVE-2022-2241**		
Affected Version(s): * Up to (excluding) 4.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	4.8	The Featured Image from URL (FIFU) WordPress plugin before 4.0.1 does not validate, sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2278**	N/A	A-FIF-FEAT-170822/834
Vendor: flask-appbuilder_project					
Product: flask-appbuilder					
Affected Version(s): * Up to (excluding) 4.1.3					
Use of Password Hash With	01-Aug-2022	2.7	Flask-AppBuilder is an application development	https://github.com/dpgaspar/Flask-	A-FLA-FLAS-170822/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insufficient Computational Effort			framework built on top of Flask python framework. In versions prior to 4.1.3 an authenticated Admin user could query other users by their salted and hashed passwords strings. These filters could be made by using partial hashed password strings. The response would not include the hashed passwords, but an attacker could infer partial password hashes and their respective users. This issue has been fixed in version 4.1.3. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31177**	AppBuilder/security/advisories/GHSA-32ff-4g79-vgfc	
Vendor: flexi_quote_rotator_project					
Product: flexi_quote_rotator					
Affected Version(s): * Up to (including) 0.9.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	4.8	The Flexi Quote Rotator WordPress plugin through 0.9.4 does not sanitise and escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting	N/A	A-FLE-FLEX-170822/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-2328**		
Vendor: Fork-cms					
Product: fork_cms					
Affected Version(s): 5.9.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2022	4.8	A stored cross-site scripting (XSS) issue in the ForkCMS version 5.9.3 allows remote attackers to inject JavaScript via the "start_date" Parameter **CVE ID : CVE-2022-35585**	https://huntr.dev/bounties/5-other-forkcms/	A-FOR-FORK-170822/837
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2022	4.8	A cross-site scripting (XSS) issue in the Fork version 5.9.3 allows remote attackers to inject JavaScript via the "publish_on_date" Parameter **CVE ID : CVE-2022-35587**	https://huntr.dev/bounties/6-other-forkcms/	A-FOR-FORK-170822/838
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2022	4.8	A cross-site scripting (XSS) issue in the Fork version 5.9.3 allows remote attackers to inject JavaScript via the "publish_on_time" Parameter. **CVE ID : CVE-2022-35589**	https://huntr.dev/bounties/7-other-forkcms/	A-FOR-FORK-170822/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-2022	4.8	A cross-site scripting (XSS) issue in the ForkCMS version 5.9.3 allows remote attackers to inject JavaScript via the "end_date" Parameter **CVE ID : CVE-2022-35590**	N/A	A-FOR-FORK-170822/840
Vendor: Fortinet					
Product: fortiadc					
Affected Version(s): 6.2.0					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): 6.2.1					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 5.0.0 Up to (excluding) 6.2.4					
Incorrect Authorization	03-Aug-2022	4.3	A unverified password change in Fortinet FortiADC version 6.2.0 through 6.2.3, 6.1.x, 6.0.x, 5.x.x allows an authenticated attacker to bypass the Old Password check in the password change form via a crafted HTTP request. **CVE ID : CVE-2022-27484**	https://fortiguard.com/psirt/FG-IR-22-055	A-FOR-FORT-170822/843
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.4					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 6.1.0 Up to (including) 6.1.6					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Product: fortimail					
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.5					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.2					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Product: fortiproxy					
Affected Version(s): 7.0.0					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): 7.0.1					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 1.0.0 Up to (including) 1.0.7					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 1.1.0 Up to (including) 1.1.6					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 1.2.0 Up to (including) 1.2.13					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 2.0.0 Up to (including) 2.0.7					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1,	https://fortiguard.com/psirt/FG-IR-21-235	A-FOR-FORT-170822/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Vendor: Foxit					
Product: pdf_editor					
Affected Version(s): * Up to (excluding) 12.0.1					
NULL Pointer Dereference	06-Aug-2022	7.5	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow a NULL pointer dereference when this.Span is used for oState of	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-170822/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Collab.addStateModel, because this.Span.text can be NULL. **CVE ID : CVE-2022-26979**		
NULL Pointer Dereference	06-Aug-2022	7.5	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow an exportXFAData NULL pointer dereference. **CVE ID : CVE-2022-27944**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-170822/855
Product: pdf_reader					
Affected Version(s): * Up to (excluding) 12.0.1					
NULL Pointer Dereference	06-Aug-2022	7.5	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow a NULL pointer dereference when this.Span is used for oState of Collab.addStateModel, because this.Span.text can be NULL. **CVE ID : CVE-2022-26979**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-170822/856
NULL Pointer Dereference	06-Aug-2022	7.5	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow an exportXFAData NULL pointer dereference. **CVE ID : CVE-2022-27944**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-170822/857
Vendor: friendsofflarum					
Product: byobu					
Affected Version(s): 0.30.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	01-Aug-2022	4.3	fof/byobu is a private discussions extension for Flarum forum. Affected versions were found to not respect private discussion disablement by users. Users of Byobu should update the extension to version 1.1.7, where this has been patched. Users of Byobu with Flarum 1.0 or 1.1 should upgrade to Flarum 1.2 or later, or evaluate the impact this issue has on your forum's users and choose to disable the extension if needed. There are no workarounds for this issue. **CVE ID : CVE-2022-35921**	https://github.com/FriendsOfFlarum/byobu/security/advisories/GHSA-6gjm-6wj6-4px5, https://github.com/FriendsOfFlarum/byobu/commit/23dcf93a30f948d30c678a96681f7fdefeba5171	A-FRI-BYOB-170822/858
Affected Version(s): From (including) 0.32.0 Up to (excluding) 1.1.7					
Improper Privilege Management	01-Aug-2022	4.3	fof/byobu is a private discussions extension for Flarum forum. Affected versions were found to not respect private discussion disablement by users. Users of Byobu should update the extension to version 1.1.7, where this has been patched. Users of	https://github.com/FriendsOfFlarum/byobu/security/advisories/GHSA-6gjm-6wj6-4px5, https://github.com/FriendsOfFlarum/byobu/commit/23dcf93a30f948d30c678a96681f7fdefeba5171	A-FRI-BYOB-170822/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Byobu with Flarum 1.0 or 1.1 should upgrade to Flarum 1.2 or later, or evaluate the impact this issue has on your forum's users and choose to disable the extension if needed. There are no workarounds for this issue. **CVE ID : CVE-2022-35921**		
Vendor: frrouting					
Product: frrouting					
Affected Version(s): 8.3					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Aug-2022	8.1	An issue was discovered in bgpd in FRRouting (FRR) 8.3. In bgp_notify_send_with_data() and bgp_process_packet() in bgp_packet.c, there is a possible use-after-free due to a race condition. This could lead to Remote Code Execution or Information Disclosure by sending crafted BGP packets. User interaction is not needed for exploitation. **CVE ID : CVE-2022-37035**	N/A	A-FRR-FRRO-170822/860
Vendor: garage_management_system_project					
Product: garage_management_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	8.8	A vulnerability was found in SourceCodester Garage Management System and classified as critical. This issue affects some unknown processing of the file removeUser.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 associated identifier of this vulnerability is VDB-205655. **CVE ID : CVE-2022-2671**	N/A	A-GAR-GARA-170822/861
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	8.8	A vulnerability was found in SourceCodester Garage Management System. It has been classified as critical. Affected is an unknown function of the file createUser.php. The manipulation of the argument userName/uemail leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to	N/A	A-GAR-GARA-170822/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. The identifier of this vulnerability is VDB-205656. **CVE ID : CVE-2022-2672**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2022	6.1	A vulnerability has been found in SourceCodester Garage Management System and classified as problematic. Affected by this vulnerability is an unknown functionality of the file edituser.php. The manipulation of the argument id with the input 1\"><ScRiPt>alert(1)</sCrIpT> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205573 was assigned to this vulnerability. **CVE ID : CVE-2022-2645**	N/A	A-GAR-GARA-170822/863
Vendor: generalized_electric_vehicle_reverse_engineering_tool_project					
Product: generalized_electric_vehicle_reverse_engineering_tool					
Affected Version(s): 2015-08-15					
Buffer Copy without Checking	03-Aug-2022	9.8	GVRET Stable Release as of Aug 15, 2015 was discovered to contain a buffer	N/A	A-GEN-GENE-170822/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			overflow via the handleConfigCmd function at SerialConsole.cpp. **CVE ID : CVE-2022-35161**		
Vendor: getlaminas					
Product: laminas-diactoros					
Affected Version(s): * Up to (excluding) 2.11.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	6.1	laminas-diactoros is a PHP package containing implementations of the PSR-7 HTTP message interfaces and PSR-17 HTTP message factory interfaces. Applications that use Diactoros, and are either not behind a proxy, or can be accessed via untrusted proxies, can potentially have the host, protocol, and/or port of a `Laminas\Diactoros\Uri` instance associated with the incoming server request modified to reflect values from `X-Forwarded-*` headers. Such changes can potentially lead to XSS attacks (if a fully-qualified URL is used in links) and/or URL poisoning. Since the `X-Forwarded-*`	https://github.com/laminas/laminas-diactoros/commit/25b11d422c2e5dad868f68619888763b30f91e2d, https://github.com/laminas/laminas-diactoros/security/advisories/GHSA-8274-h5jp-97vr	A-GET-LAMI-170822/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			headers do have valid use cases, particularly in clustered environments using a load balancer, the library offers mitigation measures only in the v2 releases, as doing otherwise would break these use cases immediately. Users of v2 releases from 2.11.1 can provide an additional argument to `Laminas\Diactoros\ServerRequestFactory::fromGlobals()` in the form of a `Laminas\Diactoros\RequestFilter\RequestFilterInterface` instance, including the shipped `Laminas\Diactoros\RequestFilter\NoOpRequestFilter` implementation which ignores the `X-Forwarded-*` headers. Starting in version 3.0, the library will reverse behavior to use the `NoOpRequestFilter` by default, and require users to opt-in to `X-Forwarded-*` header usage via a configured `Laminas\Diactoros\`		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RequestFilter\LegacyXForwardedHeaderFilter` instance. Users are advised to upgrade to version 2.11.1 or later to resolve this issue. Users unable to upgrade may configure web servers to reject `X-Forwarded-*` headers at the web server level. **CVE ID : CVE-2022-31109**		
Vendor: Github					
Product: enterprise_server					
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2022	5.4	A stored XSS vulnerability was identified in GitHub Enterprise Server that allowed the injection of arbitrary attributes. This injection was blocked by Github's Content Security Policy (CSP). This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.3.11, 3.4.6 and 3.5.3. This vulnerability was reported via the GitHub Bug Bounty program.	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.11, https://docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.3, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.6	A-GIT-ENTE-170822/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23733		
Affected Version(s): From (including) 3.4.0 Up to (excluding) 3.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2022	5.4	A stored XSS vulnerability was identified in GitHub Enterprise Server that allowed the injection of arbitrary attributes. This injection was blocked by Github's Content Security Policy (CSP). This vulnerability affected all versions of GitHub Enterprise Server prior to 3.6 and was fixed in versions 3.3.11, 3.4.6 and 3.5.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23733**	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.11, https://docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.3, https://docs.github.com/en/enterprise-server@3.4/admin/release-notes#3.4.6	A-GIT-ENTE-170822/867
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2022	5.4	A stored XSS vulnerability was identified in GitHub Enterprise Server that allowed the injection of arbitrary attributes. This injection was blocked by Github's Content Security Policy (CSP). This vulnerability affected all versions of GitHub Enterprise	https://docs.github.com/en/enterprise-server@3.3/admin/release-notes#3.3.11, https://docs.github.com/en/enterprise-server@3.5/admin/release-notes#3.5.3, https://docs.github.com/en/en	A-GIT-ENTE-170822/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server prior to 3.6 and was fixed in versions 3.3.11, 3.4.6 and 3.5.3. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2022-23733**	terprise-server@3.4/admin/release-notes#3.4.6	
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): From (including) 15.1.0 Up to (excluding) 15.1.4					
Incorrect Authorization	05-Aug-2022	8.1	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible to gain access to a private project through an email invite by using other user's email address as an unverified secondary email. **CVE ID : CVE-2022-2326**	https://gitlab.com/gitlab-org/gitlab/-/issues/356665, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2326.json	A-GIT-GITL-170822/869
Improper Privilege Management	05-Aug-2022	7.5	An issue in pipeline subscriptions in GitLab EE affecting all versions from 12.8 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 triggered new pipelines with the	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2498.json, https://gitlab.com/gitlab-	A-GIT-GITL-170822/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			person who created the tag as the pipeline creator instead of the subscription's author. **CVE ID : CVE-2022-2498**	org/gitlab/-/issues/243703	
Incorrect Authorization	05-Aug-2022	7.5	An improper access control issue in GitLab EE affecting all versions from 12.0 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an attacker to bypass IP allow-listing and download artifacts. This attack only bypasses IP allow-listing, proper permissions are still required. **CVE ID : CVE-2022-2501**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2501.json, https://gitlab.com/gitlab-org/gitlab/-/issues/364822	A-GIT-GITL-170822/871
Incorrect Authorization	05-Aug-2022	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. Membership changes are not reflected in TODO for confidential notes, allowing a former project members to	https://gitlab.com/gitlab-org/gitlab/-/issues/365742, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2512.json	A-GIT-GITL-170822/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read updates via TODOs. **CVE ID : CVE-2022-2512**		
N/A	05-Aug-2022	5.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. A malicious maintainer could exfiltrate an integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-2497**	https://gitlab.com/gitlab-org/gitlab/-/issues/362671, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2497.json	A-GIT-GITL-170822/873
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1. A stored XSS flaw in job error messages allows attackers to perform arbitrary actions on behalf of victims at client side.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2500.json, https://gitlab.com/gitlab-org/gitlab/-/issues/363725	A-GIT-GITL-170822/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2500		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	5.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.5 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was not performing correct authentication on Grafana API under specific conditions allowing unauthenticated users to perform queries through a path traversal vulnerability. **CVE ID : CVE-2022-2531**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2531.json, https://gitlab.com/gitlab-org/gitlab/-/issues/364252	A-GIT-GITL-170822/875
N/A	05-Aug-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was returning contributor emails due to improper data handling in the Datadog integration.	https://gitlab.com/gitlab-org/gitlab/-/issues/361654, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2534.json	A-GIT-GITL-170822/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2534		
Incorrect Authorization	05-Aug-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.6 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1, allowed a project member to filter issues by contact and organization. **CVE ID : CVE-2022-2539**	https://gitlab.com/gitlab-org/gitlab/-/issues/364315, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2539.json	A-GIT-GITL-170822/877
Improper Input Validation	05-Aug-2022	4.5	Insufficient validation in GitLab CE/EE affecting all versions from 12.10 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an authenticated and authorised user to import a project that includes branch names which are 40 hexadecimal characters, which could be abused in supply chain attacks where a victim pinned to a specific Git commit of the project. **CVE ID : CVE-2022-2417**	https://gitlab.com/gitlab-org/gitlab/-/issues/361179, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2417.json	A-GIT-GITL-170822/878
Incorrect Authorization	05-Aug-2022	4.3	An improper access control check in GitLab CE/EE	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-170822/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting all versions starting from 13.7 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious authenticated user to view a public project's Deploy Key's public fingerprint and name when that key has write permission. Note that GitLab never asks for nor stores the private key. **CVE ID : CVE-2022-2095**	/blob/master/2022/CVE-2022-2095.json, https://gitlab.com/gitlab-org/gitlab/-/issues/365415	
Incorrect Authorization	05-Aug-2022	4.3	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for group members to bypass 2FA enforcement enabled at the group level by using Resource Owner Password Credentials grant to obtain an access token without using 2FA.	https://gitlab.com/gitlab-org/gitlab/-/issues/355028, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2303.json	A-GIT-GITL-170822/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2303		
Authorization Bypass Through User-Controlled Key	05-Aug-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 13.10 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab's Jira integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Jira issues. **CVE ID : CVE-2022-2499**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2499.json, https://gitlab.com/gitlab-org/gitlab/-/issues/360800	A-GIT-GITL-170822/881
Incomplete Cleanup	05-Aug-2022	3.8	A lack of cascading deletes in GitLab CE/EE affecting all versions starting from 13.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious Group Owner to retain a usable Group Access Token even after the Group is deleted, though the APIs usable by that token are limited.	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2307.json, https://gitlab.com/gitlab-org/gitlab/-/issues/360025	A-GIT-GITL-170822/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2307		
Incorrect Authorization	05-Aug-2022	2.7	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for malicious group or project maintainers to change their corresponding group or project visibility by crafting a malicious POST request. **CVE ID : CVE-2022-2456**	https://gitlab.com/gitlab-org/gitlab/-/issues/359910, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2456.json	A-GIT-GITL-170822/883
Incorrect Authorization	05-Aug-2022	2.7	An issue has been discovered in GitLab EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for email invited members to join a project even after the Group Owner has enabled the setting to prevent members from being added to projects in a group, if the invite was sent	https://gitlab.com/gitlab-org/gitlab/-/issues/336169, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2459.json	A-GIT-GITL-170822/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before the setting was enabled. **CVE ID : CVE-2022-2459**		
Affected Version(s): * Up to (excluding) 15.0.5					
Incorrect Authorization	05-Aug-2022	8.1	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible to gain access to a private project through an email invite by using other user's email address as an unverified secondary email. **CVE ID : CVE-2022-2326**	https://gitlab.com/gitlab-org/gitlab/-/issues/356665, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2326.json	A-GIT-GITL-170822/885
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	5.4	A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1. A stored XSS flaw in job error messages allows attackers to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-2500**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2500.json, https://gitlab.com/gitlab-org/gitlab/-/issues/363725	A-GIT-GITL-170822/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	05-Aug-2022	4.3	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for group members to bypass 2FA enforcement enabled at the group level by using Resource Owner Password Credentials grant to obtain an access token without using 2FA. **CVE ID : CVE-2022-2303**	https://gitlab.com/gitlab-org/gitlab/-/issues/355028, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2303.json	A-GIT-GITL-170822/887
Incorrect Authorization	05-Aug-2022	2.7	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for malicious group or project maintainers to change their corresponding group or project visibility by crafting a malicious POST request.	https://gitlab.com/gitlab-org/gitlab/-/issues/359910, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2456.json	A-GIT-GITL-170822/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2456		
Incorrect Authorization	05-Aug-2022	2.7	An issue has been discovered in GitLab EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for email invited members to join a project even after the Group Owner has enabled the setting to prevent members from being added to projects in a group, if the invite was sent before the setting was enabled. **CVE ID : CVE-2022-2459**	https://gitlab.com/gitlab-org/gitlab/-/issues/336169, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2459.json	A-GIT-GITL-170822/889
Affected Version(s): 15.2					
Incorrect Authorization	05-Aug-2022	8.1	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible to gain access to a private project through an email invite by using other user's email address as an	https://gitlab.com/gitlab-org/gitlab/-/issues/356665, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2326.json	A-GIT-GITL-170822/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unverified secondary email. **CVE ID : CVE-2022-2326**		
Improper Privilege Management	05-Aug-2022	7.5	An issue in pipeline subscriptions in GitLab EE affecting all versions from 12.8 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 triggered new pipelines with the person who created the tag as the pipeline creator instead of the subscription's author. **CVE ID : CVE-2022-2498**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2498.json, https://gitlab.com/gitlab-org/gitlab/-/issues/243703	A-GIT-GITL-170822/891
Incorrect Authorization	05-Aug-2022	7.5	An improper access control issue in GitLab EE affecting all versions from 12.0 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an attacker to bypass IP allow-listing and download artifacts. This attack only bypasses IP allow-listing, proper permissions are still required. **CVE ID : CVE-2022-2501**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2501.json, https://gitlab.com/gitlab-org/gitlab/-/issues/364822	A-GIT-GITL-170822/892
Incorrect Authorization	05-Aug-2022	6.5	An issue has been discovered in GitLab CE/EE affecting all	https://gitlab.com/gitlab-org/gitlab/-	A-GIT-GITL-170822/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions starting from 15.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. Membership changes are not reflected in TODO for confidential notes, allowing a former project members to read updates via TODOs. **CVE ID : CVE-2022-2512**	/issues/365742, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2512.json	
N/A	05-Aug-2022	5.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.6 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. A malicious maintainer could exfiltrate an integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-2497**	https://gitlab.com/gitlab-org/gitlab/-/issues/362671, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2497.json	A-GIT-GITL-170822/894
Improper Neutralization of	05-Aug-2022	5.4	A cross-site scripting issue has been discovered in GitLab	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-170822/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			CE/EE affecting all versions before 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1. A stored XSS flaw in job error messages allows attackers to perform arbitrary actions on behalf of victims at client side. **CVE ID : CVE-2022-2500**	/blob/master/2022/CVE-2022-2500.json, https://gitlab.com/gitlab-org/gitlab/-/issues/363725	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	5.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.5 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was not performing correct authentication on Grafana API under specific conditions allowing unauthenticated users to perform queries through a path traversal vulnerability. **CVE ID : CVE-2022-2531**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2531.json, https://gitlab.com/gitlab-org/gitlab/-/issues/364252	A-GIT-GITL-170822/896
N/A	05-Aug-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 15.0.5, all versions	https://gitlab.com/gitlab-org/gitlab/-/issues/361654, https://gitlab.c	A-GIT-GITL-170822/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was returning contributor emails due to improper data handling in the Datadog integration. **CVE ID : CVE-2022-2534**	om/gitlab-org/cves/-/blob/master/2022/CVE-2022-2534.json	
Incorrect Authorization	05-Aug-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.6 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1, allowed a project member to filter issues by contact and organization. **CVE ID : CVE-2022-2539**	https://gitlab.com/gitlab-org/gitlab/-/issues/364315, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2539.json	A-GIT-GITL-170822/898
Improper Input Validation	05-Aug-2022	4.5	Insufficient validation in GitLab CE/EE affecting all versions from 12.10 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an authenticated and authorised user to import a project that includes branch names which are 40 hexadecimal characters, which could be abused in supply chain attacks	https://gitlab.com/gitlab-org/gitlab/-/issues/361179, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2417.json	A-GIT-GITL-170822/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where a victim pinned to a specific Git commit of the project. **CVE ID : CVE-2022-2417**		
Incorrect Authorization	05-Aug-2022	4.3	An improper access control check in GitLab CE/EE affecting all versions starting from 13.7 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious authenticated user to view a public project's Deploy Key's public fingerprint and name when that key has write permission. Note that GitLab never asks for nor stores the private key. **CVE ID : CVE-2022-2095**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2095.json, https://gitlab.com/gitlab-org/gitlab/-/issues/365415	A-GIT-GITL-170822/900
Incorrect Authorization	05-Aug-2022	4.3	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for group members to bypass	https://gitlab.com/gitlab-org/gitlab/-/issues/355028, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2303.json	A-GIT-GITL-170822/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2FA enforcement enabled at the group level by using Resource Owner Password Credentials grant to obtain an access token without using 2FA. **CVE ID : CVE-2022-2303**		
Authorization Bypass Through User-Controlled Key	05-Aug-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 13.10 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab's Jira integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Jira issues. **CVE ID : CVE-2022-2499**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2499.json, https://gitlab.com/gitlab-org/gitlab/-/issues/360800	A-GIT-GITL-170822/902
Incomplete Cleanup	05-Aug-2022	3.8	A lack of cascading deletes in GitLab CE/EE affecting all versions starting from 13.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious Group	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2307.json, https://gitlab.com/gitlab-org/gitlab/-	A-GIT-GITL-170822/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Owner to retain a usable Group Access Token even after the Group is deleted, though the APIs usable by that token are limited. **CVE ID : CVE-2022-2307**	/issues/360025	
Incorrect Authorization	05-Aug-2022	2.7	An issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for malicious group or project maintainers to change their corresponding group or project visibility by crafting a malicious POST request. **CVE ID : CVE-2022-2456**	https://gitlab.com/gitlab-org/gitlab/-/issues/359910, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2456.json	A-GIT-GITL-170822/904
Incorrect Authorization	05-Aug-2022	2.7	An issue has been discovered in GitLab EE affecting all versions before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. It may be possible for email invited members to join a project even	https://gitlab.com/gitlab-org/gitlab/-/issues/336169, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2459.json	A-GIT-GITL-170822/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after the Group Owner has enabled the setting to prevent members from being added to projects in a group, if the invite was sent before the setting was enabled. **CVE ID : CVE-2022-2459**		
Affected Version(s): From (including) 12.0.0 Up to (excluding) 15.0.5					
Incorrect Authorization	05-Aug-2022	7.5	An improper access control issue in GitLab EE affecting all versions from 12.0 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an attacker to bypass IP allow-listing and download artifacts. This attack only bypasses IP allow-listing, proper permissions are still required. **CVE ID : CVE-2022-2501**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2501.json, https://gitlab.com/gitlab-org/gitlab/-/issues/364822	A-GIT-GITL-170822/906
Affected Version(s): From (including) 12.10.0 Up to (excluding) 15.0.5					
Improper Input Validation	05-Aug-2022	4.5	Insufficient validation in GitLab CE/EE affecting all versions from 12.10 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 allows an authenticated and authorised user to import a project that	https://gitlab.com/gitlab-org/gitlab/-/issues/361179, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2417.json	A-GIT-GITL-170822/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			includes branch names which are 40 hexadecimal characters, which could be abused in supply chain attacks where a victim pinned to a specific Git commit of the project. **CVE ID : CVE-2022-2417**		
Affected Version(s): From (including) 12.5.0 Up to (excluding) 15.0.5					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	5.3	An issue has been discovered in GitLab EE affecting all versions starting from 12.5 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was not performing correct authentication on Grafana API under specific conditions allowing unauthenticated users to perform queries through a path traversal vulnerability. **CVE ID : CVE-2022-2531**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2531.json, https://gitlab.com/gitlab-org/gitlab/-/issues/364252	A-GIT-GITL-170822/908
Affected Version(s): From (including) 12.6.0 Up to (excluding) 15.0.5					
N/A	05-Aug-2022	5.5	An issue has been discovered in GitLab CE/EE affecting all versions starting	https://gitlab.com/gitlab-org/gitlab/-/issues/36267	A-GIT-GITL-170822/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 12.6 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. A malicious maintainer could exfiltrate an integration's access token by modifying the integration URL such that authenticated requests are sent to an attacker controlled server. **CVE ID : CVE-2022-2497**	1, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2497.json	
Affected Version(s): From (including) 12.8.0 Up to (excluding) 15.0.5					
Improper Privilege Management	05-Aug-2022	7.5	An issue in pipeline subscriptions in GitLab EE affecting all versions from 12.8 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1 triggered new pipelines with the person who created the tag as the pipeline creator instead of the subscription's author. **CVE ID : CVE-2022-2498**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2498.json, https://gitlab.com/gitlab-org/gitlab/-/issues/243703	A-GIT-GITL-170822/910
Affected Version(s): From (including) 13.0.0 Up to (excluding) 15.0.5					
Incomplete Cleanup	05-Aug-2022	3.8	A lack of cascading deletes in GitLab CE/EE affecting all versions starting	https://gitlab.com/gitlab-org/cves/-/blob/master/	A-GIT-GITL-170822/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 13.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious Group Owner to retain a usable Group Access Token even after the Group is deleted, though the APIs usable by that token are limited. **CVE ID : CVE-2022-2307**	2022/CVE-2022-2307.json, https://gitlab.com/gitlab-org/gitlab/-/issues/360025	
Affected Version(s): From (including) 13.10.0 Up to (excluding) 15.0.5					
Authorization Bypass Through User-Controlled Key	05-Aug-2022	4.3	An issue has been discovered in GitLab EE affecting all versions starting from 13.10 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab's Jira integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Jira issues. **CVE ID : CVE-2022-2499**	https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2499.json, https://gitlab.com/gitlab-org/gitlab/-/issues/360800	A-GIT-GITL-170822/912
Affected Version(s): From (including) 13.7.0 Up to (excluding) 15.0.5					
Incorrect Authorization	05-Aug-2022	4.3	An improper access control check in GitLab CE/EE	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-170822/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting all versions starting from 13.7 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1 allows a malicious authenticated user to view a public project's Deploy Key's public fingerprint and name when that key has write permission. Note that GitLab never asks for nor stores the private key. **CVE ID : CVE-2022-2095**	/blob/master/2022/CVE-2022-2095.json, https://gitlab.com/gitlab-org/gitlab/-/issues/365415	
Affected Version(s): From (including) 14.6.0 Up to (excluding) 15.0.5					
Incorrect Authorization	05-Aug-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 14.6 prior to 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1, allowed a project member to filter issues by contact and organization. **CVE ID : CVE-2022-2539**	https://gitlab.com/gitlab-org/gitlab/-/issues/364315, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2539.json	A-GIT-GITL-170822/914
Affected Version(s): From (including) 15.0.0 Up to (excluding) 15.0.5					
Incorrect Authorization	05-Aug-2022	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting	https://gitlab.com/gitlab-org/gitlab/-/issues/36574	A-GIT-GITL-170822/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from 15.0 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. Membership changes are not reflected in TODO for confidential notes, allowing a former project members to read updates via TODOs. **CVE ID : CVE-2022-2512**	2, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2512.json	
Affected Version(s): From (including) 9.3.0 Up to (excluding) 15.0.5					
N/A	05-Aug-2022	5.3	An issue has been discovered in GitLab CE/EE affecting all versions starting from 9.3 before 15.0.5, all versions starting from 15.1 before 15.1.4, all versions starting from 15.2 before 15.2.1. GitLab was returning contributor emails due to improper data handling in the Datadog integration. **CVE ID : CVE-2022-2534**	https://gitlab.com/gitlab-org/gitlab/-/issues/361654, https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2534.json	A-GIT-GITL-170822/916
Vendor: givewp					
Product: givewp					
Affected Version(s): * Up to (excluding) 2.21.3					
Cross-Site Request	01-Aug-2022	6.5	The GiveWP WordPress plugin before 2.21.3 does	N/A	A-GIV-GIVE-170822/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			not have CSRF in place when exporting data, and does not validate the exporting parameters such as dates, which could allow attackers to make a logged in admin DoS the web server via a CSRF attack as the plugin will try to retrieve data from the database many times which leads to overwhelm the target's CPU. **CVE ID : CVE-2022-2260**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	4.8	The GiveWP WordPress plugin before 2.21.3 does not properly sanitise and escape the currency settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2215**	N/A	A-GIV-GIVE-170822/918
Vendor: GNU					
Product: gnutls					
Affected Version(s): * Up to (excluding) 3.7.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	01-Aug-2022	7.5	A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verification of pkcs7 signatures in gnutls_pkcs7_verify function. **CVE ID : CVE-2022-2509**	https://lists.gnupg.org/pipermail/gnutls-help/2022-July/004746.html	A-GNU-GNUT-170822/919
Vendor: Golang					
Product: go					
Affected Version(s): * Up to (excluding) 1.17.11					
Improper Control of Generation of Code ('Code Injection')	10-Aug-2022	7.8	Code injection in Cmd.Start in os/exec before Go 1.17.11 and Go 1.18.3 allows execution of any binaries in the working directory named either "..com" or "..exe" by calling Cmd.Run, Cmd.Start, Cmd.Output, or Cmd.CombinedOutput when Cmd.Path is unset. **CVE ID : CVE-2022-30580**	https://go.dev/cl/403759, https://go.googlesource.com/go/+/960ffa98ce73ef2c2060c84c7ac28d37a83f345e, https://pkg.go.dev/vuln/GO-2022-0532	A-GOL-GO-170822/920
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Aug-2022	7.5	Incorrect conversion of certain invalid paths to valid, absolute paths in Clean in path/filepath before Go 1.17.11 and Go 1.18.3 on Windows allows potential	https://go.googlesource.com/go/+/9cd1818a7d019c02fa4898b3e45a323e35033290, https://groups.google.com/g/golang-announce/c/TzIC9-	A-GOL-GO-170822/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			directory traversal attack. **CVE ID : CVE-2022-29804**	t8Ytg/m/IWz5T6x7AAAJ, https://pkg.go.dev/vuln/GO-2022-0533, https://go.dev/cl/401595, https://go.dev/issue/52476	
Affected Version(s): * Up to (excluding) 1.17.12					
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Decoder.Skip in encoding/xml before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a deeply nested XML document. **CVE ID : CVE-2022-28131**	https://pkg.go.dev/vuln/GO-2022-0521, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE, https://go.googlesource.com/go/+/08c46ed43d80bbb67cb904944ea3417989be4af3, https://go.dev/issue/53614, https://go.dev/cl/417062	A-GOL-GO-170822/922
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Glob in io/fs before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path which contains a large number of path separators. **CVE ID : CVE-2022-30630**	https://go.dev/cl/417065, https://go.googlesource.com/go/+/fa2d41d0ca736f3ad6b200b2a4e134364e9acc59, https://pkg.go.dev/vuln/GO-2022-0527, https://go.dev/issue/53415, https://groups.google.com/g/	A-GOL-GO-170822/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				golang-announce/c/nqrv9fbR0zE	
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Reader.Read in compress/gzip before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via an archive containing a large number of concatenated 0-length compressed files. **CVE ID : CVE-2022-30631**	https://pkg.go.dev/vuln/GO-2022-0524, https://go.googlesource.com/go/+/b2b8872c876201eac2d0707276c6999ff3eb185e, https://go.dev/cl/417067, https://go.dev/issue/53168, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	A-GOL-GO-170822/924
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Glob in path/filepath before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path containing a large number of path separators. **CVE ID : CVE-2022-30632**	https://go.dev/issue/53416, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE, https://pkg.go.dev/vuln/GO-2022-0522, https://go.dev/cl/417066, https://go.googlesource.com/go/+/ac68c6c683409f98250d34ad282b9e1b0c9095ef	A-GOL-GO-170822/925
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Unmarshal in encoding/xml before	https://go.googlesource.com/go/+/c4c1993fd2a5b26fe45c09	A-GOL-GO-170822/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via unmarshalling an XML document into a Go struct which has a nested field that uses the 'any' field tag. **CVE ID : CVE-2022-30633**	592af6d3388a3b2e08, https://go.dev/cl/417061, https://go.dev/issue/53611, https://pkg.go.dev/vuln/GO-2022-0523, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Decoder.Decode in encoding/gob before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a message which contains deeply nested structures. **CVE ID : CVE-2022-30635**	https://go.dev/cl/417064, https://go.googlesource.com/go/+/6fa37e98ea4382bf881428ee0c150ce591500eb7, https://pkg.go.dev/vuln/GO-2022-0526, https://go.dev/issue/53615, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	A-GOL-GO-170822/927
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	10-Aug-2022	6.5	Acceptance of some invalid Transfer-Encoding headers in the HTTP/1 client in net/http before Go 1.17.12 and Go 1.18.4 allows HTTP request smuggling if combined with an intermediate server that also improperly	https://go.dev/cl/409874, https://pkg.go.dev/vuln/GO-2022-0525, https://go.googlesource.com/go/+/e5017a93fcde94f09836200bca55324af037ee5f,	A-GOL-GO-170822/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fails to reject the header as invalid. **CVE ID : CVE-2022-1705**	https://go.dev/cl/410714, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE, https://go.dev/issue/53188	
N/A	10-Aug-2022	6.5	Improper exposure of client IP addresses in net/http before Go 1.17.12 and Go 1.18.4 can be triggered by calling httputil.ReverseProxy.ServeHTTP with a Request.Header map containing a nil value for the X-Forwarded-For header, which causes ReverseProxy to set the client IP as the value of the X-Forwarded-For header. **CVE ID : CVE-2022-32148**	https://go.dev/cl/412857, https://go.googlesource.com/go/+/b2cc0fecc2ccd80e6d5d16542cc684f97b3a9c8a, https://pkg.go.dev/vuln/GO-2022-0520	A-GOL-GO-170822/929
Uncontrolled Recursion	10-Aug-2022	5.5	Uncontrolled recursion in the Parse functions in go/parser before Go 1.17.12 and Go 1.18.4 allow an attacker to cause a panic due to stack exhaustion via deeply nested types or declarations. **CVE ID : CVE-2022-1962**	https://go.dev/cl/417063, https://go.googlesource.com/go/+/695be961d57508da5a82217f7415200a11845879, https://pkg.go.dev/vuln/GO-2022-0515, https://go.dev/issue/53616, https://groups.google.com/g/	A-GOL-GO-170822/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				golang-announce/c/nqrv9fbR0zE	
Affected Version(s): * Up to (excluding) 1.17.13					
N/A	10-Aug-2022	7.5	A too-short encoded message can cause a panic in Float.GobDecode and Rat GobDecode in math/big in Go before 1.17.13 and 1.18.5, potentially allowing a denial of service. **CVE ID : CVE-2022-32189**	https://pkg.go.dev/vuln/GO-2022-0537, https://go.dev/cl/417774, https://go.googlesource.com/go/+/055113ef364337607e3e72ed7d48df67fde6fc66	A-GOL-GO-170822/931
Affected Version(s): From (including) 1.18.0 Up to (excluding) 1.18.3					
Improper Control of Generation of Code ('Code Injection')	10-Aug-2022	7.8	Code injection in Cmd.Start in os/exec before Go 1.17.11 and Go 1.18.3 allows execution of any binaries in the working directory named either "..com" or "..exe" by calling Cmd.Run, Cmd.Start, Cmd.Output, or Cmd.CombinedOutput when Cmd.Path is unset. **CVE ID : CVE-2022-30580**	https://go.dev/cl/403759, https://go.googlesource.com/go/+/960ffa98ce73ef2c2060c84c7ac28d37a83f345e, https://pkg.go.dev/vuln/GO-2022-0532	A-GOL-GO-170822/932
Improper Limitation of a Pathname to a Restricted Directory	10-Aug-2022	7.5	Incorrect conversion of certain invalid paths to valid, absolute paths in Clean in path/filepath before Go 1.17.11 and Go 1.18.3 on Windows allows potential	https://go.googlesource.com/go/+/9cd1818a7d019c02fa4898b3e45a323e35033290, https://groups.google.com/g/golang-	A-GOL-GO-170822/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			directory traversal attack. **CVE ID : CVE-2022-29804**	announce/c/TzIC9-t8Ytg/m/IWz5T6x7AAAJ, https://pkg.go.dev/vuln/GO-2022-0533, https://go.dev/cl/401595, https://go.dev/issue/52476	
Affected Version(s): From (including) 1.18.0 Up to (excluding) 1.18.4					
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Decoder.Skip in encoding/xml before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a deeply nested XML document. **CVE ID : CVE-2022-28131**	https://pkg.go.dev/vuln/GO-2022-0521, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE, https://go.googlesource.com/go/+/08c46ed43d80bbb67cb904944ea3417989be4af3, https://go.dev/issue/53614, https://go.dev/cl/417062	A-GOL-GO-170822/934
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Glob in io/fs before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path which contains a large number of path separators.	https://go.dev/cl/417065, https://go.googlesource.com/go/+/fa2d41d0ca736f3ad6b200b2a4e134364e9acc59, https://pkg.go.dev/vuln/GO-2022-0527, https://go.dev/issue/53415,	A-GOL-GO-170822/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30630	https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Reader.Read in compress/gzip before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via an archive containing a large number of concatenated 0-length compressed files. **CVE ID : CVE-2022-30631**	https://pkg.go.dev/vuln/GO-2022-0524, https://go.googlesource.com/go/+/b2b8872c876201eac2d0707276c6999ff3eb185e, https://go.dev/cl/417067, https://go.dev/issue/53168, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	A-GOL-GO-170822/936
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Glob in path/filepath before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path containing a large number of path separators. **CVE ID : CVE-2022-30632**	https://go.dev/issue/53416, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE, https://pkg.go.dev/vuln/GO-2022-0522, https://go.dev/cl/417066, https://go.googlesource.com/go/+/ac68c6c683409f98250d34ad282b9e1b0c9095ef	A-GOL-GO-170822/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Unmarshal in encoding/xml before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via unmarshalling an XML document into a Go struct which has a nested field that uses the 'any' field tag. **CVE ID : CVE-2022-30633**	https://go.googlesource.com/go/+/c4c1993fd2a5b26fe45c09592af6d3388a3b2e08, https://go.dev/cl/417061, https://go.dev/issue/53611, https://pkg.go.dev/vuln/GO-2022-0523, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	A-GOL-GO-170822/938
Uncontrolled Recursion	10-Aug-2022	7.5	Uncontrolled recursion in Decoder.Decode in encoding/gob before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a message which contains deeply nested structures. **CVE ID : CVE-2022-30635**	https://go.dev/cl/417064, https://go.googlesource.com/go/+/6fa37e98ea4382bf881428ee0c150ce591500eb7, https://pkg.go.dev/vuln/GO-2022-0526, https://go.dev/issue/53615, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	A-GOL-GO-170822/939
Inconsistent Interpretation of HTTP Requests ('HTTP	10-Aug-2022	6.5	Acceptance of some invalid Transfer-Encoding headers in the HTTP/1 client in net/http before Go 1.17.12 and Go 1.18.4 allows HTTP	https://go.dev/cl/409874, https://pkg.go.dev/vuln/GO-2022-0525, https://go.googlesource.com/g	A-GOL-GO-170822/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Smuggling')			request smuggling if combined with an intermediate server that also improperly fails to reject the header as invalid. **CVE ID : CVE-2022-1705**	o/+/e5017a93fcde94f09836200bca55324af037ee5f, https://go.dev/cl/410714, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE, https://go.dev/issue/53188	
N/A	10-Aug-2022	6.5	Improper exposure of client IP addresses in net/http before Go 1.17.12 and Go 1.18.4 can be triggered by calling httputil.ReverseProxy.ServeHTTP with a Request.Header map containing a nil value for the X-Forwarded-For header, which causes ReverseProxy to set the client IP as the value of the X-Forwarded-For header. **CVE ID : CVE-2022-32148**	https://go.dev/cl/412857, https://go.googlesource.com/go/+/b2cc0fecc2ccd80e6d5d16542cc684f97b3a9c8a, https://pkg.go.dev/vuln/GO-2022-0520	A-GOL-GO-170822/941
Uncontrolled Recursion	10-Aug-2022	5.5	Uncontrolled recursion in the Parse functions in go/parser before Go 1.17.12 and Go 1.18.4 allow an attacker to cause a panic due to stack exhaustion via deeply nested types or declarations.	https://go.dev/cl/417063, https://go.googlesource.com/go/+/695be961d57508da5a82217f7415200a11845879, https://pkg.go.dev/vuln/GO-2022-0515,	A-GOL-GO-170822/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1962	https://go.dev/issue/53616, https://groups.google.com/g/golang-announce/c/nqrv9fbR0zE	
Affected Version(s): From (including) 1.18.0 Up to (excluding) 1.18.5					
N/A	10-Aug-2022	7.5	A too-short encoded message can cause a panic in Float.GobDecode and Rat GobDecode in math/big in Go before 1.17.13 and 1.18.5, potentially allowing a denial of service. **CVE ID : CVE-2022-32189**	https://pkg.go.dev/vuln/GO-2022-0537, https://go.dev/cl/417774, https://go.googlesource.com/go/+/055113ef364337607e3e72ed7d48df67fde6fc66	A-GOL-GO-170822/943
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 102.0.5005.125					
Out-of-bounds Write	12-Aug-2022	9.8	Out of bounds write in Chrome OS Audio Server in Google Chrome on Chrome OS prior to 102.0.5005.125 allowed a remote attacker to potentially exploit heap corruption via crafted audio metadata. **CVE ID : CVE-2022-2587**	https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-chromeos.html, https://crbug.com/1320917	A-GOO-CHRO-170822/944
Affected Version(s): * Up to (excluding) 104.0.5112.79					
Use After Free	12-Aug-2022	8.8	Use after free in Omnibox in Google Chrome prior to	https://chromereleases.googleblog.com/2022	A-GOO-CHRO-170822/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2603**	/08/stable-channel-update-for-desktop.html, https://crbug.com/1325699	
Use After Free	12-Aug-2022	8.8	Use after free in Safe Browsing in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2604**	https://crbug.com/1335316, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/946
Use After Free	12-Aug-2022	8.8	Use after free in Managed devices API in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to enable a specific Enterprise policy to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2606**	https://crbug.com/1330489, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/947
Use After Free	12-Aug-2022	8.8	Use after free in Tab Strip in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to	https://crbug.com/1286203, https://chromereleases.googleblog.com/2022/08/stable-channel-	A-GOO-CHRO-170822/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2607**	update-for-desktop.html	
Use After Free	12-Aug-2022	8.8	Use after free in Overview Mode in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2608**	https://crbug.com/1330775, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/949
Use After Free	12-Aug-2022	8.8	Use after free in Nearby Share in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2609**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1338560	A-GOO-CHRO-170822/950
Use After Free	12-Aug-2022	8.8	Use after free in Input in Google	https://chromerereleases.google	A-GOO-CHRO-170822/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to enage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2613**	blog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1325256	
Use After Free	12-Aug-2022	8.8	Use after free in Sign-In Flow in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2614**	https://crbug.com/1341907, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/952
Use After Free	12-Aug-2022	8.8	Use after free in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2617**	https://crbug.com/1292451, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/953
Use After Free	12-Aug-2022	8.8	Use after free in WebUI in Google Chrome on Chrome	https://crbug.com/1337304, https://chrome	A-GOO-CHRO-170822/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2620**	releases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	
Use After Free	12-Aug-2022	8.8	Use after free in Extensions in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2621**	https://crbug.com/1323449, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/955
Use After Free	12-Aug-2022	8.8	Use after free in Offline in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1337798	A-GOO-CHRO-170822/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2623		
Out-of-bounds Write	12-Aug-2022	8.8	Heap buffer overflow in PDF in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2022-2624**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1339745	A-GOO-CHRO-170822/957
Out-of-bounds Read	12-Aug-2022	6.5	Out of bounds read in Dawn in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2022-2605**	https://crbug.com/1338470, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/958
Exposure of Resource to Wrong Sphere	12-Aug-2022	6.5	Insufficient policy enforcement in Background Fetch in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2022-2610**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1278255	A-GOO-CHRO-170822/959
Observable Discrepancy	12-Aug-2022	6.5	Side-channel information leakage in Keyboard input in Google Chrome prior	https://chromereleases.googleblog.com/2022/08/stable-	A-GOO-CHRO-170822/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to 104.0.5112.79 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2022-2612**	channel-update-for-desktop.html, https://crbug.com/1321350	
Reliance on Cookies without Validation and Integrity Checking	12-Aug-2022	6.5	Insufficient policy enforcement in Cookies in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2022-2615**	https://crbug.com/1268580, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	A-GOO-CHRO-170822/961
N/A	12-Aug-2022	6.5	Inappropriate implementation in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to spoof the contents of the Omnibox (URL bar) via a crafted Chrome Extension. **CVE ID : CVE-2022-2616**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1302159	A-GOO-CHRO-170822/962
Improper Input Validation	12-Aug-2022	6.5	Insufficient validation of untrusted input in Internals in Google	https://crbug.com/1308422, https://chromereleases.google	A-GOO-CHRO-170822/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Chrome prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a malicious file . **CVE ID : CVE-2022-2618**	blog.com/2022/08/stable-channel-update-for-desktop.html	
Improper Input Validation	12-Aug-2022	6.5	Insufficient validation of untrusted input in Safe Browsing in Google Chrome on Windows prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a crafted file. **CVE ID : CVE-2022-2622**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1332392	A-GOO-CHRO-170822/964
N/A	12-Aug-2022	4.3	Inappropriate implementation in Fullscreen API in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2022-2611**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1320538	A-GOO-CHRO-170822/965
Improper Input Validation	12-Aug-2022	4.3	Insufficient validation of untrusted input in Settings in Google Chrome prior to	https://crbug.com/1332881, https://chromereleases.googleblog.com/2022	A-GOO-CHRO-170822/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted HTML page. **CVE ID : CVE-2022-2619**	/08/stable-channel-update-for-desktop.html	
Vendor: google_maps_anywhere_project					
Product: google_maps_anywhere					
Affected Version(s): * Up to (including) 1.2.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The Google Maps Anywhere WordPress plugin through 1.2.6.3 does not sanitise and escape any of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2424**	N/A	A-GOO-GOOG-170822/967
Vendor: graphql-go_project					
Product: graphql-go					
Affected Version(s): * Up to (including) 0.8.0					
Uncontrolled Recursion	01-Aug-2022	7.5	graphql-go (aka GraphQL for Go) through 0.8.0 has infinite recursion in	N/A	A-GRA-GRAP-170822/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the type definition parser. **CVE ID : CVE-2022-37315**		
Vendor: grommunio					
Product: gromox					
Affected Version(s): From (including) 0.5 Up to (excluding) 1.28					
Incorrect Default Permissions	04-Aug-2022	7.8	Weak permissions on the configuration file in the PAM module in Grommunio Gromox 0.5 through 1.x before 1.28 allow a local unprivileged user in the gromox group to have the PAM stack execute arbitrary code upon loading the Gromox PAM module. **CVE ID : CVE-2022-37030**	N/A	A-GRO-GROM-170822/969
Vendor: gym_management_system_project					
Product: gym_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-2022	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System. Affected is an unknown function. The manipulation of the argument user_pass leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to	N/A	A-GYM-GYM_-170822/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. VDB-205734 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2687**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System. This affects an unknown part of the file login.php. The manipulation of the argument user_login with the input 123@xx.com' OR (SELECT 9084 FROM(SELECT COUNT(*),CONCAT(0x7178767871,(SELECT (ELT(9084=9084,1))),0x71767a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- dPvW leads to sql injection. Access to the local network is required for this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-205833 was assigned to this vulnerability.	N/A	A-GYM-GYM_-170822/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2708		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2022	9.8	A vulnerability was found in SourceCodester Gym Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /mygym/admin/login.php. The manipulation of the argument admin_email/admin_pass 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-205855. **CVE ID : CVE-2022-2727**	N/A	A-GYM-GYM_-170822/972
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2022	9.8	A vulnerability was found in SourceCodester Gym Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file /mygym/admin/index.php. The manipulation of the argument edit_tran	N/A	A-GYM-GYM_-170822/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC 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-205856. **CVE ID : CVE-2022-2728**		
Unrestricted Upload of File with Dangerous Type	11-Aug-2022	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester Gym Management System. Affected by this issue is some unknown functionality of the file /admin/add_exercises.php of the component Background Management. The manipulation of the argument exer_img leads to unrestricted upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-206012. **CVE ID : CVE-2022-2744**	N/A	A-GYM-GYM_-170822/974
Improper Neutralization of Special Elements used in an	11-Aug-2022	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System. This affects	N/A	A-GYM-GYM_-170822/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			an unknown part of the file /admin/add_trainers.php of the component Add New Trainer. The manipulation of the argument trainer_name leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-206013 was assigned to this vulnerability. **CVE ID : CVE-2022-2745**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	8.8	A vulnerability classified as critical has been found in SourceCodester Gym Management System. This affects an unknown part of the component GET Parameter Handler. The manipulation of the argument day 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-205821 was assigned to this vulnerability. **CVE ID : CVE-2022-2700**	N/A	A-GYM-GYM_-170822/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	8.8	A vulnerability was found in SourceCodester Gym Management System. It has been classified as critical. This affects an unknown part of the component Exercises Module. The manipulation of the argument exer 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-205827. **CVE ID : CVE-2022-2703**	N/A	A-GYM-GYM_-170822/977
Unrestricted Upload of File with Dangerous Type	11-Aug-2022	8.8	A vulnerability was found in SourceCodester Gym Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /mygym/admin/index.php?view_exercises. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may	N/A	A-GYM-GYM_-170822/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The identifier VDB-206017 was assigned to this vulnerability. **CVE ID : CVE-2022-2749**		
N/A	11-Aug-2022	5.3	A vulnerability classified as problematic has been found in SourceCodester Gym Management System. Affected is an unknown function of the file delete_user.php. The manipulation of the argument delete_user leads to denial of service. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-206172. **CVE ID : CVE-2022-2776**	N/A	A-GYM-GYM_-170822/979
Vendor: hcltechsw					
Product: hcl_launch					
Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 7.0.5.12					
Incorrect Authorization	03-Aug-2022	6.5	HCL Launch could allow an authenticated user to obtain sensitive information in some instances due to improper security checking. **CVE ID : CVE-2022-27551**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099732	A-HCL-HCL_-170822/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 7.1.0.0 Up to (excluding) 7.1.2.8					
Incorrect Authorization	03-Aug-2022	6.5	HCL Launch could allow an authenticated user to obtain sensitive information in some instances due to improper security checking. **CVE ID : CVE-2022-27551**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099732	A-HCL-HCL_-170822/981
Affected Version(s): From (including) 7.2.0.0 Up to (excluding) 7.2.3.1					
Incorrect Authorization	03-Aug-2022	6.5	HCL Launch could allow an authenticated user to obtain sensitive information in some instances due to improper security checking. **CVE ID : CVE-2022-27551**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0099732	A-HCL-HCL_-170822/982
Vendor: hestiacp					
Product: control_panel					
Affected Version(s): * Up to (excluding) 1.6.6					
Improper Input Validation	05-Aug-2022	8.8	Improper Input Validation in GitHub repository hestiacp/hestiacp prior to 1.6.6. **CVE ID : CVE-2022-2636**	https://huntr.dev/bounties/357c0390-631c-4684-b6e1-a6d8b2453d66, https://github.com/hestiacp/hestiacp/commit/b178b9719bb2c98cf8a6db70065086f596afad81	A-HES-CONT-170822/983
Incorrect Privilege	05-Aug-2022	7.2	Incorrect Privilege Assignment in GitHub repository	https://github.com/hestiacp/hestiacp/comm	A-HES-CONT-170822/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Assignment			hestiacp/hestiacp prior to 1.6.6. **CVE ID : CVE-2022-2626**	it/b178b9719bb2c98cf8a6db70065086f596aad81, https://huntr.dev/bounties/704aacc9-edff-4da5-90a6-4adf8dbf36fe	
Vendor: hinet					
Product: hicos_natural_person_credential_component_client					
Affected Version(s): 3.0.3.30306					
Out-of-bounds Write	02-Aug-2022	6.8	HiCOS Citizen verification component has a stack-based buffer overflow vulnerability due to insufficient parameter length validation. An unauthenticated physical attacker can exploit this vulnerability to execute arbitrary code, manipulate system command or disrupt service. **CVE ID : CVE-2022-35222**	N/A	A-HIN-HICO-170822/985
Affected Version(s): 3.0.3.30404					
Out-of-bounds Write	02-Aug-2022	6.8	HiCOS Citizen verification component has a stack-based buffer overflow vulnerability due to insufficient parameter length validation. An unauthenticated	N/A	A-HIN-HICO-170822/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			physical attacker can exploit this vulnerability to execute arbitrary code, manipulate system command or disrupt service. **CVE ID : CVE-2022-35222**		
Affected Version(s): 3.1.0.00002					
Out-of-bounds Write	02-Aug-2022	6.8	HiCOS Citizen verification component has a stack-based buffer overflow vulnerability due to insufficient parameter length validation. An unauthenticated physical attacker can exploit this vulnerability to execute arbitrary code, manipulate system command or disrupt service. **CVE ID : CVE-2022-35222**	N/A	A-HIN-HICO-170822/987
Vendor: IBM					
Product: cics_tx					
Affected Version(s): 11.1					
Cross-Site Request Forgery (CSRF)	01-Aug-2022	8.8	IBM CICS TX 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website	https://www.ibm.com/support/pages/node/6608194, https://exchange.xforce.ibmcloud.com/vulnerabilities/229331,	A-IBM-CICS-170822/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trusts. IBM X-Force ID: 229331. **CVE ID : CVE-2022-34161**	https://www.ibm.com/support/pages/node/6608192	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-Aug-2022	6.8	IBM CICS TX 11.1 could allow allow an attacker with physical access to the system to execute code due using a back and refresh attack. IBM X-Force ID: 229312. **CVE ID : CVE-2022-33955**	https://www.ibm.com/support/pages/node/6608190, https://exchange.xforce.ibmcloud.com/vulnerabilities/229312, https://www.ibm.com/support/pages/node/6608186	A-IBM-CICS-170822/989
Improper Restriction of Rendered UI Layers or Frames	01-Aug-2022	6.1	IBM CICS TX 11.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 229332. **CVE ID : CVE-2022-34162**	https://www.ibm.com/support/pages/node/6608198, https://www.ibm.com/support/pages/node/6608196, https://exchange.xforce.ibmcloud.com/vulnerabilities/229332	A-IBM-CICS-170822/990
Improper Neutralization of Input During	01-Aug-2022	6.1	IBM CICS TX 11.1 is vulnerable to HTTP header injection, caused by improper validation of input by	https://www.ibm.com/support/pages/node/6608202, https://www.i	A-IBM-CICS-170822/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 229333. **CVE ID : CVE-2022-34163**	bm.com/support/pages/node/6608200, https://exchange.xforce.ibmcloud.com/vulnerabilities/229333	
Improper Input Validation	01-Aug-2022	5.5	IBM CICS TX 11.1 could allow a local user to impersonate another legitimate user due to improper input validation. IBM X-Force ID: 229338. **CVE ID : CVE-2022-34164**	https://www.ibm.com/support/pages/node/6608206, https://www.ibm.com/support/pages/node/6608204, https://exchange.xforce.ibmcloud.com/vulnerabilities/229338	A-IBM-CICS-170822/992
Incorrect Authorization	01-Aug-2022	4.3	IBM CICS TX 11.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping	https://exchange.xforce.ibmcloud.com/vulnerabilities/229436, https://www.ibm.com/support/pages/node/6608210, https://www.ibm.com/support/pages/node/6608208	A-IBM-CICS-170822/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the traffic. IBM X-Force ID: 229436. **CVE ID : CVE-2022-34307**		
Product: datapower_gateway					
Affected Version(s): 10.5.0.0					
Improper Restriction of XML External Entity Reference	01-Aug-2022	9.1	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228359. **CVE ID : CVE-2022-31775**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228359, https://www.ibm.com/support/pages/node/6608608	A-IBM-DATA-170822/994
Server-Side Request Forgery (SSRF)	01-Aug-2022	8.8	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized	https://exchange.xforce.ibmcloud.com/vulnerabilities/228433, https://www.ibm.com/support/pages/node/6608604	A-IBM-DATA-170822/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 228433. **CVE ID : CVE-2022-31776**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228358. **CVE ID : CVE-2022-31774**	https://www.ibm.com/support/pages/node/6608600, https://exchange.xforce.ibmcloud.com/vulnerabilities/228358	A-IBM-DATA-170822/996
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 is vulnerable to cross-site scripting. This vulnerability allows users to	https://www.ibm.com/support/pages/node/6608600, https://exchange.xforce.ibmcloud.com/vulnerabilities/228435	A-IBM-DATA-170822/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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: 228435. **CVE ID : CVE-2022-32750**		
Affected Version(s): From (including) 10.0.1.0 Up to (excluding) 10.0.1.6					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	A-IBM-DATA-170822/998
Affected Version(s): From (including) 10.0.1.0 Up to (excluding) 10.0.1.8					
Improper Restriction of XML External Entity Reference	01-Aug-2022	9.1	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data.	https://exchange.xforce.ibmcloud.com/vulnerabilities/228359, https://www.ibm.com/support/pages/node/6608608	A-IBM-DATA-170822/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 228359. **CVE ID : CVE-2022-31775**		
Affected Version(s): From (including) 10.0.1.0 Up to (including) 10.0.1.8					
Server-Side Request Forgery (SSRF)	01-Aug-2022	8.8	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 228433. **CVE ID : CVE-2022-31776**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228433, https://www.ibm.com/support/pages/node/6608604	A-IBM-DATA-170822/1000
Improper Neutralization of Input During Web Page Generation	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 is vulnerable to	https://www.ibm.com/support/pages/node/6608600, https://exchange.xforce.ibmcloud.com/vulne	A-IBM-DATA-170822/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('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: 228358. **CVE ID : CVE-2022-31774**	rabilities/228358	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228435. **CVE ID : CVE-2022-32750**	https://www.ibm.com/support/pages/node/6608600, https://exchange.xforce.ibmcloud.com/vulnerabilities/228435	A-IBM-DATA-170822/1002
Affected Version(s): From (including) 10.0.2.0 Up to (excluding) 10.0.5.0					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0,	https://www.ibm.com/support/pages/node	A-IBM-DATA-170822/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	
Affected Version(s): From (including) 10.0.2.0 Up to (excluding) 10.5.0.1					
Improper Restriction of XML External Entity Reference	01-Aug-2022	9.1	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228359. **CVE ID : CVE-2022-31775**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228359, https://www.ibm.com/support/pages/node/6608608	A-IBM-DATA-170822/1004
Server-Side Request Forgery (SSRF)	01-Aug-2022	8.8	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0	https://exchange.xforce.ibmcloud.com/vulnerabilities/228433, https://www.i	A-IBM-DATA-170822/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 2018.4.1.21 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 228433. **CVE ID : CVE-2022-31776**	bm.com/support/pages/node/6608604	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228358. **CVE ID : CVE-2022-31774**	https://www.ibm.com/support/pages/node/6608600, https://exchange.xforce.ibmcloud.com/vulnerabilities/228358	A-IBM-DATA-170822/1006
Improper Neutralization of	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0,	https://www.ibm.com/support/pages/node	A-IBM-DATA-170822/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228435. **CVE ID : CVE-2022-32750**	/6608600, https://exchange.xforce.ibmcloud.com/vulnerabilities/228435	
Affected Version(s): From (including) 2018.4.1.0 Up to (excluding) 2018.4.1.19					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	A-IBM-DATA-170822/1008
Affected Version(s): From (including) 2018.4.1.0 Up to (excluding) 2018.4.1.21					
Improper Restriction of XML External	01-Aug-2022	9.1	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through	https://exchange.xforce.ibmcloud.com/vulnerabilities/2283	A-IBM-DATA-170822/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228359. **CVE ID : CVE-2022-31775**	59, https://www.ibm.com/support/pages/node/6608608	
Affected Version(s): From (including) 2018.4.1.0 Up to (including) 2018.4.1.21					
Server-Side Request Forgery (SSRF)	01-Aug-2022	8.8	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 228433. **CVE ID : CVE-2022-31776**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228433, https://www.ibm.com/support/pages/node/6608604	A-IBM-DATA-170822/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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: 228358. **CVE ID : CVE-2022-31774**	https://www.ibm.com/support/pages/node/6608600, https://exchange.xforce.ibmcloud.com/vulnerabilities/228358	A-IBM-DATA-170822/1011
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	5.4	IBM DataPower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.8, 10.5.0.0, and 2018.4.1.0 through 2018.4.1.21 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	https://www.ibm.com/support/pages/node/6608600, https://exchange.xforce.ibmcloud.com/vulnerabilities/228435	A-IBM-DATA-170822/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trusted session. IBM X-Force ID: 228435. **CVE ID : CVE-2022-32750**		
Product: infosphere_information_server					
Affected Version(s): 11.7					
Generation of Error Message Containing Sensitive Information	10-Aug-2022	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in a stack trace. This information could be used in further attacks against the system. IBM X-Force ID: 231202. **CVE ID : CVE-2022-35715**	https://exchange.xforce.ibmcloud.com/vulnerabilities/231202, https://www.ibm.com/support/pages/node/6610883	A-IBM-INFO-170822/1013
Product: robotic_process_automation					
Affected Version(s): * Up to (excluding) 21.0.3					
Files or Directories Accessible to External Parties	10-Aug-2022	4.9	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a privileged user to obtain sensitive Azure bot credential information. IBM X-Force ID: 226342. **CVE ID : CVE-2022-22490**	https://www.ibm.com/support/pages/node/6610397, https://exchange.xforce.ibmcloud.com/vulnerabilities/226342	A-IBM-ROBO-170822/1014
Affected Version(s): 21.0.0					
Exposure of Resource	01-Aug-2022	4.3	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2	https://www.ibm.com/support/pages/node	A-IBM-ROBO-170822/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			could allow a user to access information from a tenant of which they should not have access. IBM X-Force ID: 219391. **CVE ID : CVE-2022-22334**	/6608550, https://exchange.xforce.ibmcloud.com/vulnerabilities/219391	
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.0.3					
N/A	01-Aug-2022	7.5	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 contains a vulnerability that could allow IBM tenant credentials to be exposed. IBM X-Force ID: 227288. **CVE ID : CVE-2022-22505**	https://www.ibm.com/support/pages/node/6608404, https://exchange.xforce.ibmcloud.com/vulnerabilities/227288	A-IBM-ROBO-170822/1016
Improper Privilege Management	01-Aug-2022	7.2	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a privileged user to elevate their privilege to platform administrator through manipulation of APIs. IBM X-Force ID: 227978. **CVE ID : CVE-2022-30616**	https://exchange.xforce.ibmcloud.com/vulnerabilities/227978, https://www.ibm.com/support/pages/node/6608430	A-IBM-ROBO-170822/1017
Improper Privilege Management	01-Aug-2022	6.5	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could disclose sensitive information due to improper privilege management for	https://exchange.xforce.ibmcloud.com/vulnerabilities/229962, https://www.ibm.com/suppo	A-IBM-ROBO-170822/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			storage provider types. IBM X-Force ID: 229962. **CVE ID : CVE-2022-34338**	rt/pages/node/6608606	
Affected Version(s): From (including) 21.0.0 Up to (including) 21.0.3					
Insufficiently Protected Credentials	01-Aug-2022	6.5	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 is vulnerable to insufficiently protected credentials for users created via a bulk upload. IBM X-Force ID: 228888. **CVE ID : CVE-2022-33169**	https://exchange.xforce.ibmcloud.com/vulnerabilities/228888, https://www.ibm.com/support/pages/node/6608454	A-IBM-ROBO-170822/1019
Affected Version(s): From (including) 21.0.1 Up to (excluding) 21.0.1.7					
Exposure of Resource to Wrong Sphere	01-Aug-2022	4.3	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user to access information from a tenant of which they should not have access. IBM X-Force ID: 219391. **CVE ID : CVE-2022-22334**	https://www.ibm.com/support/pages/node/6608550, https://exchange.xforce.ibmcloud.com/vulnerabilities/219391	A-IBM-ROBO-170822/1020
Affected Version(s): From (including) 21.0.2 Up to (excluding) 21.0.2.5					
Exposure of Resource to Wrong Sphere	01-Aug-2022	4.3	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a user to access information from a tenant of which they should not have access. IBM X-Force ID: 219391.	https://www.ibm.com/support/pages/node/6608550, https://exchange.xforce.ibmcloud.com/vulnerabilities/219391	A-IBM-ROBO-170822/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22334		
Product: robotic_process_automation_as_a_service					
Affected Version(s): *					
Files or Directories Accessible to External Parties	10-Aug-2022	4.9	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a privileged user to obtain sensitive Azure bot credential information. IBM X-Force ID: 226342. **CVE ID : CVE-2022-22490**	https://www.ibm.com/support/pages/node/6610397, https://exchange.xforce.ibmcloud.com/vulnerabilities/226342	A-IBM-ROBO-170822/1022
Product: robotic_process_automation_for_cloud_pak					
Affected Version(s): * Up to (excluding) 21.0.3					
Files or Directories Accessible to External Parties	10-Aug-2022	4.9	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a privileged user to obtain sensitive Azure bot credential information. IBM X-Force ID: 226342. **CVE ID : CVE-2022-22490**	https://www.ibm.com/support/pages/node/6610397, https://exchange.xforce.ibmcloud.com/vulnerabilities/226342	A-IBM-ROBO-170822/1023
Affected Version(s): 21.0.0					
Weak Password Requirements	10-Aug-2022	9.8	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 230634.	https://www.ibm.com/support/pages/node/6610393	A-IBM-ROBO-170822/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35280		
Affected Version(s): 21.0.1					
Weak Password Requirements	10-Aug-2022	9.8	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 230634. **CVE ID : CVE-2022-35280**	https://www.ibm.com/support/pages/node/6610393	A-IBM-ROBO-170822/1025
Affected Version(s): 21.0.2					
Weak Password Requirements	10-Aug-2022	9.8	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 230634. **CVE ID : CVE-2022-35280**	https://www.ibm.com/support/pages/node/6610393	A-IBM-ROBO-170822/1026
Product: urbancode_deploy					
Affected Version(s): From (including) 7.0.0.0 Up to (excluding) 7.0.5.12					
Exposure of Resource to Wrong Sphere	01-Aug-2022	6.5	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.16, 7.0.0.0 through 7.0.5.11, 7.1.0.0 through 7.1.2.7, and 7.2.0.0 through 7.2.3.0 could allow an authenticated	https://exchange.xforce.ibmcloud.com/vulnerabilities/231360, https://www.ibm.com/support/pages/node/6608584	A-IBM-URBA-170822/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to obtain sensitive information in some instances due to improper security checking. IBM X-Force ID: 231360. **CVE ID : CVE-2022-35716**		
Affected Version(s): From (including) 7.1.0.0 Up to (excluding) 7.1.2.8					
Exposure of Resource to Wrong Sphere	01-Aug-2022	6.5	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.16, 7.0.0.0 through 7.0.5.11, 7.1.0.0 through 7.1.2.7, and 7.2.0.0 through 7.2.3.0 could allow an authenticated user to obtain sensitive information in some instances due to improper security checking. IBM X-Force ID: 231360. **CVE ID : CVE-2022-35716**	https://exchange.xforce.ibmcloud.com/vulnerabilities/231360, https://www.ibm.com/support/pages/node/6608584	A-IBM-URBA-170822/1028
Affected Version(s): From (including) 7.2.0.0 Up to (excluding) 7.2.3.1					
Exposure of Resource to Wrong Sphere	01-Aug-2022	6.5	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.16, 7.0.0.0 through 7.0.5.11, 7.1.0.0 through 7.1.2.7, and 7.2.0.0 through 7.2.3.0 could allow an authenticated user to obtain sensitive information in some instances due to improper	https://exchange.xforce.ibmcloud.com/vulnerabilities/231360, https://www.ibm.com/support/pages/node/6608584	A-IBM-URBA-170822/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security checking. IBM X-Force ID: 231360. **CVE ID : CVE-2022-35716**		
Affected Version(s): From (including) 6.2.0.0 Up to (excluding) 6.2.7.17					
Exposure of Resource to Wrong Sphere	01-Aug-2022	6.5	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.16, 7.0.0.0 through 7.0.5.11, 7.1.0.0 through 7.1.2.7, and 7.2.0.0 through 7.2.3.0 could allow an authenticated user to obtain sensitive information in some instances due to improper security checking. IBM X-Force ID: 231360. **CVE ID : CVE-2022-35716**	https://exchange.xforce.ibmcloud.com/vulnerabilities/231360, https://www.ibm.com/support/pages/node/6608584	A-IBM-URBA-170822/1030
Product: workload_scheduler					
Affected Version(s): 9.4					
N/A	10-Aug-2022	7.1	IBM Workload Scheduler 9.4 and 9.5 could allow a local user to overwrite key system files which would cause the system to crash. IBM X-Force ID: 221187. **CVE ID : CVE-2022-22369**	https://exchange.xforce.ibmcloud.com/vulnerabilities/221187, https://www.ibm.com/support/pages/node/6610903	A-IBM-WORK-170822/1031
Affected Version(s): 9.5					
N/A	10-Aug-2022	7.1	IBM Workload Scheduler 9.4 and 9.5 could allow a	https://exchange.xforce.ibmcloud.com/vulne	A-IBM-WORK-170822/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local user to overwrite key system files which would cause the system to crash. IBM X-Force ID: 221187. **CVE ID : CVE-2022-22369**	rabilities/221187, https://www.ibm.com/support/pages/node/6610903	
Vendor: ideastocode					
Product: enable_svg\,_webp_\&_ico_upload					
Affected Version(s): * Up to (including) 1.0.1					
Unrestricted Upload of File with Dangerous Type	01-Aug-2022	8.8	Authenticated (author or higher user role) Arbitrary File Upload vulnerability in ideasToCode Enable SVG, WebP & ICO Upload plugin <= 1.0.1 at WordPress. **CVE ID : CVE-2022-34154**	https://patchstack.com/database/vulnerability/enable-svg-webp-ico-upload/wordpress-enable-svg-webp-ico-upload-plugin-1-0-1-authenticated-arbitrary-file-upload-vulnerability, https://wordpress.org/plugins/enable-svg-webp-ico-upload/#developers	A-IDE-ENAB-170822/1033
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	5.4	Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in ideasToCode Enable SVG, WebP & ICO Upload plugin <= 1.0.1 at WordPress.	https://patchstack.com/database/vulnerability/enable-svg-webp-ico-upload/wordpress-enable-svg-webp-ico-upload-plugin-1-0-1-authenticated-	A-IDE-ENAB-170822/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36343	stored-cross-site-scripting-xss-vulnerability, https://wordpress.org/plugins/enable-svg-webp-ico-upload/#developers	
Vendor: Inductiveautomation					
Product: ignition					
Affected Version(s): From (including) 7.9.0 Up to (excluding) 7.9.21					
Improper Restriction of XML External Entity Reference	05-Aug-2022	9.8	Due to an XML external entity reference, the software parses XML in the backup/restore functionality without XML security flags, which may lead to a XXE attack while restoring the backup. **CVE ID : CVE-2022-1704**	N/A	A-IND-IGNI-170822/1035
Affected Version(s): From (including) 8.1.0 Up to (excluding) 8.1.8					
Improper Restriction of XML External Entity Reference	05-Aug-2022	9.8	Due to an XML external entity reference, the software parses XML in the backup/restore functionality without XML security flags, which may lead to a XXE attack while restoring the backup. **CVE ID : CVE-2022-1704**	N/A	A-IND-IGNI-170822/1036
Vendor: inglorion					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: muhttpd					
Affected Version(s): * Up to (excluding) 1.1.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**	N/A	A-ING-MUHT-170822/1037
Vendor: Intel					
Product: connman					
Affected Version(s): * Up to (including) 1.41					
Out-of-bounds Write	03-Aug-2022	9.8	In ConnMan through 1.41, remote attackers able to send HTTP requests to the gweb component are able to exploit a heap-based buffer overflow in received_data to execute code. **CVE ID : CVE-2022-32292**	https://lore.kernel.org/connman/20220801080043.4861-5-wagi@monom.org/	A-INT-CONN-170822/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Aug-2022	8.1	In ConnMan through 1.41, a man-in-the-middle attack against a WISPR HTTP query could be used to trigger a use-after-free in WISPR handling, leading to crashes or code execution. **CVE ID : CVE-2022-32293**	https://lore.kernel.org/connman/20220801080043.4861-3-wagi@monom.org/, https://lore.kernel.org/connman/20220801080043.4861-1-wagi@monom.org/, https://bugzilla.suse.com/show_bug.cgi?id=1200190	A-INT-CONN-170822/1039
Vendor: interview_management_system_project					
Product: interview_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	9.8	A vulnerability was found in SourceCodester Interview Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /viewReport.php. The manipulation of the argument id with the input (UPDATEXML(9729,CONCAT(0x2e,0x716b707071,(SELECT(ELT(9729=9729,1))),0x7162766a71),7319)) leads to sql injection. The attack may be initiated	N/A	A-INT-INTE-170822/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-205667. **CVE ID : CVE-2022-2679**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	A vulnerability was found in SourceCodester Interview Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /addQuestion.php. The manipulation of the argument question with the input <script>alert(1)</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 identifier VDB-205673 was assigned to this vulnerability. **CVE ID : CVE-2022-2685**	N/A	A-INT-INTE-170822/1041
Vendor: ittiam					
Product: libmpeg2					
Affected Version(s): * Up to (excluding) 2022-07-27					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Aug-2022	6.5	Ittiam libmpeg2 before 2022-07-27 uses memcpy with overlapping memory blocks in impeg2_mc_fullx_fully_8x8. **CVE ID : CVE-2022-37416**	N/A	A-ITT-LIBM-170822/1042
Vendor: jeecg					
Product: jeecg_boot					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	04-Aug-2022	9.8	A vulnerability was found in jeecg-boot. It has been declared as critical. This vulnerability affects unknown code of the file /api/. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-205594 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2647**	N/A	A-JEE-JEEC-170822/1043
Vendor: Jetbrains					
Product: rider					
Affected Version(s): * Up to (excluding) 2022.2					
N/A	03-Aug-2022	7.8	In JetBrains Rider before 2022.2 Trust and Open Project dialog could be	https://www.jetbrains.com/privacy-	A-JET-RIDE-170822/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassed, leading to local code execution **CVE ID : CVE-2022-37396**	security/issues-fixed/	
Product: teamcity					
Affected Version(s): * Up to (excluding) 2022.04.3					
Insertion of Sensitive Information into Log File	10-Aug-2022	5.3	In JetBrains TeamCity before 2022.04.3 the private SSH key could be written to the server log in some cases **CVE ID : CVE-2022-38133**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-170822/1045
Vendor: jflyfox					
Product: jfinal_cms					
Affected Version(s): 5.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	8.8	JFinal CMS v5.1.0 was discovered to contain a SQL injection vulnerability via /system/user. **CVE ID : CVE-2022-34928**	N/A	A-JFL-JFIN-170822/1046
Vendor: joinbookwyrm					
Product: bookwyrm					
Affected Version(s): * Up to (excluding) 0.4.5					
Authentication Bypass by Primary Weakness	04-Aug-2022	9.8	Authentication Bypass by Primary Weakness in GitHub repository bookwyrm-social/bookwyrm prior to 0.4.5.	https://huntr.dev/bounties/428eee94-f1a0-45d0-9e25-318641115550, https://github.com/bookwyr	A-JOI-BOOK-170822/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2651	m-social/bookwyrm/commit/7bbe42fb30a79a26115524d18b697d895563c92f	
Improper Authentication	02-Aug-2022	9.8	BookWyrm is a social network for tracking reading. Versions prior to 0.4.5 were found to lack rate limiting on authentication views which allows brute-force attacks. This issue has been patched in version 0.4.5. Admins with existing instances will need to update their `nginx.conf` file that was created when the instance was set up. Users are advised advised to upgrade. Users unable to upgrade may update their nginx.conf files with the changes manually. **CVE ID : CVE-2022-35925**	https://www.github.com/bookwyrm-social/bookwyrm/commit/7bbe42fb30a79a26115524d18b697d895563c92f, https://github.com/bookwyrm-social/bookwyrm/security/advisories/GHSA-jvp3-mqv8-5rjw	A-JOI-BOOK-170822/1048
Vendor: jumpdemand					
Product: activedemand					
Affected Version(s): * Up to (including) 0.2.27					
Improper Authentication	05-Aug-2022	5.3	Broken Authentication vulnerability in JumpDEMAND Inc. ActiveDEMAND plugin <= 0.2.27 at	https://wordpress.org/plugins/activedemand/#developers, https://patchstack.com/datab	A-JUM-ACTI-170822/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress allows unauthenticated post update/create/delete. **CVE ID : CVE-2022-36296**	ase/vulnerability/activedemand/wordpress-activedemand-plugin-0-2-27-broken-authentication-vulnerability	
Vendor: juniper_project					
Product: juniper					
Affected Version(s): * Up to (excluding) 0.15.10					
Uncontrolled Resource Consumption	01-Aug-2022	7.5	Juniper is a GraphQL server library for Rust. Affected versions of Juniper are vulnerable to uncontrolled recursion resulting in a program crash. This issue has been addressed in version 0.15.10. Users are advised to upgrade. Users unable to upgrade should limit the recursion depth manually. **CVE ID : CVE-2022-31173**	https://github.com/graphql-rust/juniper/commit/8d28cdba6eb10f53490ba41d1b5cb40506c2de22, https://github.com/graphql-rust/juniper/commit/2b609ee057be950e3454b69fadc431d120e407bb	A-JUN-JUNI-170822/1050
Vendor: kainelabs					
Product: youzify					
Affected Version(s): * Up to (excluding) 1.2.0					
Improper Neutralization of Special Elements used in an SQL Command	01-Aug-2022	9.8	The Youzify WordPress plugin before 1.2.0 does not sanitise and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated	N/A	A-KAI-YOUZ-170822/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			users, leading to an unauthenticated SQL injection **CVE ID : CVE-2022-1950**		
Vendor: Kaspersky					
Product: vpn_secure_connection					
Affected Version(s): * Up to (excluding) 21.6					
N/A	05-Aug-2022	7.8	Kaspersky VPN Secure Connection for Windows version up to 21.5 was vulnerable to arbitrary file deletion via abuse of its 'Delete All Service Data And Reports' feature by the local authenticated attacker. **CVE ID : CVE-2022-27535**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#050822, https://forum.kaspersky.com/topic/kaspersky-statement-on-cve-2022-27535-26742/	A-KAS-VPN_-170822/1052
Vendor: kava					
Product: kava					
Affected Version(s): * Up to (excluding) 0.18.0					
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.3	Ethermint is an Ethereum library. In Ethermint running versions before `v0.17.2`, the contract `selfdestruct` invocation permanently removes the corresponding bytecode from the internal database storage. However, due to a bug in the `DeleteAccount`funct	https://github.com/evmos/ethermint/commit/144741832007a26dbe950512acbda4ed95b2a451, https://github.com/evmos/ethermint/security/advisories/GHSA-f92v-grc2-w2fg	A-KAV-KAVA-170822/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ion, all contracts that used the identical bytecode (i.e shared the same `CodeHash`) will also stop working once one contract invokes `selfdestruct`, even though the other contracts did not invoke the `selfdestruct` OPCODE. This vulnerability has been patched in Ethermint version v0.18.0. The patch has state machine-breaking changes for applications using Ethermint, so a coordinated upgrade procedure is required. A workaround is available. If a contract is subject to DoS due to this issue, the user can redeploy the same contract, i.e. with identical bytecode, so that the original contract's code is recovered. The new contract deployment restores the `bytecode hash -> bytecode` entry in the internal state. **CVE ID : CVE-2022-35936**		
Vendor: kavita					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: kavita					
Affected Version(s): * Up to (excluding) 0.5.4.1					
Server-Side Request Forgery (SSRF)	10-Aug-2022	6.5	Server-Side Request Forgery (SSRF) in GitHub repository kareadita/kavita prior to 0.5.4.1. **CVE ID : CVE-2022-2756**	https://github.com/kareadita/kavita/commit/9c31f7e7c81b919923cb2e3857439ec0d16243e4, https://huntr.dev/bounties/95e7c181-9d80-4428-aebf-687ac55a9216	A-KAV-KAVI-170822/1054
Vendor: keysight					
Product: sensor_management_server					
Affected Version(s): 2.4.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Aug-2022	9.8	A path traversal vulnerability exists in the com.keysight.tentacle.licensing.LicenseManager.addLicenseFile() method in the Keysight Sensor Management Server (SMS). This allows an unauthenticated remote attacker to upload arbitrary files to the SMS host. **CVE ID : CVE-2022-38129**	N/A	A-KEY-SENS-170822/1055
Improper Neutralization of Special Elements used in an SQL Command	10-Aug-2022	9.8	The com.keysight.tentacle.config.ResourceManager.smsRestoreDatabaseZip() method is used to restore the HSQLDB database used in SMS. It takes	N/A	A-KEY-SENS-170822/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			the path of the zipped database file as the single parameter. An unauthenticated, remote attacker can specify an UNC path for the database file (i.e., \\<attacker-host>\sms\<attacker-db.zip>), effectively controlling the content of the database to be restored. **CVE ID : CVE-2022-38130**		
Vendor: krakend					
Product: krakend					
Affected Version(s): * Up to (excluding) 2.0.0					
N/A	01-Aug-2022	4.3	Lura and KrakenD-CE versions older than v2.0.2 and KrakenD-EE versions older than v2.0.0 do not sanitize URL parameters correctly, allowing a malicious user to alter the backend URL defined for a pipe when remote users send crafty URL requests. The vulnerability does not affect KrakenD itself, but the consumed backend might be vulnerable. **CVE ID : CVE-2022-1561**	https://www.krakend.io/blog/cve-2022-1561-crafted-backend-urls/, https://www.incibe-cert.es/en/early-warning/security-advisories/crafted-backend-urls-lura-project	A-KRA-KRAK-170822/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.0.2					
N/A	01-Aug-2022	4.3	Lura and KrakenD-CE versions older than v2.0.2 and KrakenD-EE versions older than v2.0.0 do not sanitize URL parameters correctly, allowing a malicious user to alter the backend URL defined for a pipe when remote users send crafty URL requests. The vulnerability does not affect KrakenD itself, but the consumed backend might be vulnerable. **CVE ID : CVE-2022-1561**	https://www.krakend.io/blog/cve-2022-1561-crafted-backend-urls/, https://www.incibe-cert.es/en/early-warning/security-advisories/crafted-backend-urls-lura-project	A-KRA-KRAK-170822/1058
Vendor: kromit					
Product: titra					
Affected Version(s): * Up to (excluding) 0.79.1					
Improper Authorization	01-Aug-2022	10	Improper Authorization in GitHub repository kromitgmbh/titra prior to 0.79.1. **CVE ID : CVE-2022-2595**	https://github.com/kromitgmbh/titra/commit/fe8c3cdeb70e53b9f38f1022186ab16324d332c5, https://huntr.dev/bounties/1c6afb84-2025-46d8-9e9f-cbfc20e5d04d	A-KRO-TITR-170822/1059
Vendor: kuka					
Product: systemsoftware_v\/kss					
Affected Version(s): From (including) 8.2 Up to (excluding) 8.6.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	10-Aug-2022	9.8	The KUKA SystemSoftware V/KSS in versions prior to 8.6.5 is prone to improper access control as an unauthorized attacker can directly read and write robot configurations when access control is not available or not enabled (default). **CVE ID : CVE-2022-2242**	https://www.kuka.com/advisories-CVE-2022-2242	A-KUK-SYST-170822/1060
Vendor: landray					
Product: landray_office_automation					
Affected Version(s): -					
Cleartext Storage of Sensitive Information	02-Aug-2022	7.5	Lanling OA Landray Office Automation (OA) internal patch number #133383/#137780 contains an arbitrary file read vulnerability via the component /sys/ui/extend/varkind/custom.jsp. **CVE ID : CVE-2022-34924**	N/A	A-LAN-LAND-170822/1061
Vendor: library_management_system_project					
Product: library_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Library Management System. It has been declared as critical. This vulnerability	N/A	A-LIB-LIBR-170822/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			affects unknown code of the file librarian/student.php. The manipulation of the argument title leads to sql injection. The attack can be initiated remotely. VDB-206170 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2774**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-2022	6.1	A vulnerability classified as problematic was found in SourceCodester Library Management System. This vulnerability affects unknown code of the file /qr/I/. The manipulation of the argument error leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-206164. **CVE ID : CVE-2022-2768**	N/A	A-LIB-LIBR-170822/1063
Vendor: loan_management_system_project					
Product: loan_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Loan Management System. It has been rated as	N/A	A-LOA-LOAN-170822/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			critical. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-206162 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2766**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	8.8	A vulnerability was found in SourceCodester Loan Management System and classified as critical. This issue affects some unknown processing of the file delete_lplan.php. The manipulation of the argument lplan_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-205619. **CVE ID : CVE-2022-2667**	N/A	A-LOA-LOAN-170822/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: login_with_phone_number_project					
Product: login_with_phone_number					
Affected Version(s): * Up to (including) 1.3.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	4.8	The Login with phone number WordPress plugin before 1.3.8 does not sanitise and escape plugin settings which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-0598**	N/A	A-LOG-LOGI-170822/1066
Vendor: luadec_project					
Product: luadec					
Affected Version(s): 0.9.9					
Out-of-bounds Write	03-Aug-2022	7.8	Luadec v0.9.9 was discovered to contain a heap-buffer overflow via the function UnsetPending. **CVE ID : CVE-2022-34992**	N/A	A-LUA-LUAD-170822/1067
Vendor: luraproject					
Product: lura					
Affected Version(s): * Up to (excluding) 2.0.2					
N/A	01-Aug-2022	4.3	Lura and KrakenD-CE versions older than v2.0.2 and KrakenD-EE versions older than v2.0.0 do not sanitize URL	https://www.krakend.io/blog/cve-2022-1561-crafted-backend-urls/, https://www.i	A-LUR-LURA-170822/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters correctly, allowing a malicious user to alter the backend URL defined for a pipe when remote users send crafty URL requests. The vulnerability does not affect KrakenD itself, but the consumed backend might be vulnerable. **CVE ID : CVE-2022-1561**	ncibe-cert.es/en/early-warning/security-advisories/crafted-backend-urls-lura-project	
Vendor: mailerlite					
Product: mailerlite_signup_forms					
Affected Version(s): * Up to (excluding) 1.5.8					
Cross-Site Request Forgery (CSRF)	05-Aug-2022	8.8	Cross-Site Request Forgery (CSRF) vulnerability in MailerLite – Signup forms (official) plugin <= 1.5.7 at WordPress allows an attacker to change the API key. **CVE ID : CVE-2022-33201**	https://wordpress.org/plugins/official-mailerlite-sign-up-forms/#developers	A-MAI-MAIL-170822/1069
Vendor: makedp					
Product: mprweb					
Affected Version(s): * Up to (including) 5.0.0					
Exposure of Sensitive Information to an Unauthorized Actor	01-Aug-2022	5.3	mprweb is a hosting platform for the makedeb Package Repository. Email addresses were found to not have been hidden, even if a user had clicked the `Hide Email	https://github.com/makedeb/mprweb/commit/d13e3f2f5a9c0b0f6782f35d837090732026ad77, https://github.com/makedeb/	A-MAK-MPRW-170822/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Address` checkbox on their account page, or during signup. This could lead to an account's email being leaked, which may be problematic if your email needs to remain private for any reason. Users hosting their own mprweb instance will need to upgrade to the latest commit to get this fixed. Users on the official instance will already have this issue fixed. **CVE ID : CVE-2022-31185**	mprweb/security/advisories/GHSA-jm39-h693-678g	
Vendor: mc-kill-port_project					
Product: mc-kill-port					
Affected Version(s): *					
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	10-Aug-2022	7.8	All versions of package mc-kill-port are vulnerable to Arbitrary Command Execution via the kill function, due to missing sanitization of the port argument. **CVE ID : CVE-2022-25973**	https://security.snyk.io/vuln/SNYK-JS-MCKILLPORT-2419070, https://www.npmjs.com/package/mc-kill-port	A-MC--MC-K-170822/1071
Vendor: mealie_project					
Product: mealie					
Affected Version(s): 0.5.5					
Improper Neutralization of Input	02-Aug-2022	5.4	A stored cross-site scripting (XSS) vulnerability in Mealie v0.5.5 allows	N/A	A-MEA-MEAL-170822/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Shopping Lists item names text field. **CVE ID : CVE-2022-34619**		
Affected Version(s): 1.0.0					
Unrestricted Upload of File with Dangerous Type	02-Aug-2022	9.8	Mealie 1.0.0beta3 contains an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via a crafted file. **CVE ID : CVE-2022-34613**	https://docs.mealie.io/changelog/v0.5.6/	A-MEA-MEAL-170822/1073
Improper Control of Generation of Code ('Code Injection')	02-Aug-2022	7.2	Mealie1.0.0beta3 was discovered to contain a Server-Side Template Injection vulnerability, which allows attackers to execute arbitrary code via a crafted Jinja2 template. **CVE ID : CVE-2022-34625**	https://docs.mealie.io/changelog/v0.5.6/	A-MEA-MEAL-170822/1074
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2022	5.4	A stored cross-site scripting (XSS) vulnerability in Mealie 1.0.0beta3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the	N/A	A-MEA-MEAL-170822/1075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			recipe description text field. **CVE ID : CVE-2022-34618**		
Vendor: mediajedi					
Product: user_private_files					
Affected Version(s): * Up to (excluding) 1.1.3					
Unrestricted Upload of File with Dangerous Type	08-Aug-2022	8.8	The Frontend File Manager & Sharing WordPress plugin before 1.1.3 does not filter file extensions when letting users upload files on the server, which may lead to malicious code being uploaded. **CVE ID : CVE-2022-2356**	N/A	A-MED-USER-170822/1076
Vendor: mediatek					
Product: nbiot_sdk					
Affected Version(s): 2.8.1					
Out-of-bounds Write	01-Aug-2022	9.8	In httpclient, there is a possible out of bounds write due to uninitialized data. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WSAP00103831; Issue ID: WSAP00103831. **CVE ID : CVE-2022-26437**	https://corp.mediatek.com/product-security-bulletin/August-2022	A-MED-NBIO-170822/1077
Vendor: Microsoft					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: .net					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.8					
N/A	09-Aug-2022	5.9	.NET Spoofing Vulnerability. **CVE ID : CVE-2022-34716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34716	A-MIC-.NET-170822/1078
Product: .net_core					
Affected Version(s): From (including) 3.1 Up to (excluding) 3.1.28					
N/A	09-Aug-2022	5.9	.NET Spoofing Vulnerability. **CVE ID : CVE-2022-34716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34716	A-MIC-.NET-170822/1079
Product: 365_apps					
Affected Version(s): -					
N/A	09-Aug-2022	8.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34717	A-MIC-365_-170822/1080
N/A	09-Aug-2022	7.3	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-33631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33631	A-MIC-365_-170822/1081
Product: azure_batch					
Affected Version(s): * Up to (excluding) 1.9.27					
N/A	09-Aug-2022	7	Azure Batch Node Agent Elevation of	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-AZUR-170822/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-33646**	guidance/advisory/CVE-2022-33646	
Product: azure_real_time_operating_system_guix_studio					
Affected Version(s): -					
N/A	09-Aug-2022	7.8	Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-30176, CVE-2022-34687, CVE-2022-35773, CVE-2022-35779, CVE-2022-35806. **CVE ID : CVE-2022-30175**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30175	A-MIC-AZUR-170822/1083
N/A	09-Aug-2022	7.8	Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-30175, CVE-2022-34687, CVE-2022-35773, CVE-2022-35779, CVE-2022-35806. **CVE ID : CVE-2022-30176**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30176	A-MIC-AZUR-170822/1084
N/A	09-Aug-2022	7.8	Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-30175, CVE-2022-30176, CVE-2022-35773, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34687	A-MIC-AZUR-170822/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35779, CVE-2022-35806. **CVE ID : CVE-2022-34687**		
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	7.8	Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-30175, CVE-2022-30176, CVE-2022-34687, CVE-2022-35779, CVE-2022-35806. **CVE ID : CVE-2022-35773**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35773	A-MIC-AZUR-170822/1086
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	7.8	Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-30175, CVE-2022-30176, CVE-2022-34687, CVE-2022-35773, CVE-2022-35806. **CVE ID : CVE-2022-35779**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35779	A-MIC-AZUR-170822/1087
N/A	09-Aug-2022	7.8	Azure RTOS GUIX Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-30175, CVE-2022-30176, CVE-2022-34687, CVE-2022-35773, CVE-2022-35779.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35806	A-MIC-AZUR-170822/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35806		
N/A	09-Aug-2022	5.5	Azure RTOS GUIX Studio Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34686. **CVE ID : CVE-2022-34685**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34685	A-MIC-AZUR-170822/1089
N/A	09-Aug-2022	5.5	Azure RTOS GUIX Studio Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34685. **CVE ID : CVE-2022-34686**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34686	A-MIC-AZUR-170822/1090
Product: azure_site_recovery					
Affected Version(s): * Up to (excluding) 9.50.6419.1					
N/A	09-Aug-2022	8.1	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35802	A-MIC-AZUR-170822/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35800, CVE-2022-35801, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35802**		
N/A	09-Aug-2022	7.2	Azure Site Recovery Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35772. **CVE ID : CVE-2022-35824**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35824	A-MIC-AZUR-170822/1092
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35799	A-MIC-AZUR-170822/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35790, CVE-2022-35791, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35799**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35802, CVE-2022-35807, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35801	A-MIC-AZUR-170822/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35801**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35807	A-MIC-AZUR-170822/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35807**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35808	A-MIC-AZUR-170822/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35808		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35809**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35809	A-MIC-AZUR-170822/1097
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-AZUR-170822/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35810**	guidance/advisory/CVE-2022-35810	
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35811	A-MIC-AZUR-170822/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35811**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35813	A-MIC-AZUR-170822/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35813**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35814	A-MIC-AZUR-170822/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35814**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35815	A-MIC-AZUR-170822/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35815**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35817, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35816	A-MIC-AZUR-170822/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35818, CVE-2022-35819. **CVE ID : CVE-2022-35816**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35817**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35817	A-MIC-AZUR-170822/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35819. **CVE ID : CVE-2022-35818**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35818	A-MIC-AZUR-170822/1105
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-AZUR-170822/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818. **CVE ID : CVE-2022-35819**	ory/CVE-2022-35819	
N/A	09-Aug-2022	4.9	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35800	A-MIC-AZUR-170822/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35800**		
N/A	09-Aug-2022	4.9	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35812	A-MIC-AZUR-170822/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35812**		
Product: azure_site_recovery_vmware_to_azure					
Affected Version(s): * Up to (excluding) 9.50.6419.1					
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	7.2	Azure Site Recovery Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35824. **CVE ID : CVE-2022-35772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35772	A-MIC-AZUR-170822/1109
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35775	A-MIC-AZUR-170822/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35775**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35780	A-MIC-AZUR-170822/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35780**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35781	A-MIC-AZUR-170822/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35781**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35782	A-MIC-AZUR-170822/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35782**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35784	A-MIC-AZUR-170822/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35784		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35785**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35785	A-MIC-AZUR-170822/1115
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-AZUR-170822/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35786**	guidance/advisory/CVE-2022-35786	
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35788	A-MIC-AZUR-170822/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35788**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35789	A-MIC-AZUR-170822/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35789**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35790	A-MIC-AZUR-170822/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35790**		
N/A	09-Aug-2022	6.5	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35791	A-MIC-AZUR-170822/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35791**		
N/A	09-Aug-2022	6.2	Azure Site Recovery Denial of Service Vulnerability. **CVE ID : CVE-2022-35776**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35776	A-MIC-AZUR-170822/1121
N/A	09-Aug-2022	4.9	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35774	A-MIC-AZUR-170822/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35774**		
N/A	09-Aug-2022	4.9	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35783, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35787	A-MIC-AZUR-170822/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35818, CVE-2022-35819. **CVE ID : CVE-2022-35787**		
N/A	09-Aug-2022	4.4	Azure Site Recovery Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35774, CVE-2022-35775, CVE-2022-35780, CVE-2022-35781, CVE-2022-35782, CVE-2022-35784, CVE-2022-35785, CVE-2022-35786, CVE-2022-35787, CVE-2022-35788, CVE-2022-35789, CVE-2022-35790, CVE-2022-35791, CVE-2022-35799, CVE-2022-35800, CVE-2022-35801, CVE-2022-35802, CVE-2022-35807, CVE-2022-35808, CVE-2022-35809, CVE-2022-35810, CVE-2022-35811, CVE-2022-35812, CVE-2022-35813, CVE-2022-35814, CVE-2022-35815, CVE-2022-35816, CVE-2022-35817, CVE-2022-35818, CVE-2022-35819. **CVE ID : CVE-2022-35783**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35783	A-MIC-AZUR-170822/1124
Product: azure_sphere					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 22.07					
N/A	09-Aug-2022	4.4	Azure Sphere Information Disclosure Vulnerability. **CVE ID : CVE-2022-35821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35821	A-MIC-AZUR-170822/1125
Product: edge_chromium					
Affected Version(s): * Up to (excluding) 104.0.1293.47					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.3	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33636**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33636	A-MIC-EDGE-170822/1126
N/A	09-Aug-2022	8.3	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-33649**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33649	A-MIC-EDGE-170822/1127
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.5	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35796**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35796	A-MIC-EDGE-170822/1128
Product: excel					
Affected Version(s): 2013					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.3	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-33631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33631	A-MIC-EXCE-170822/1129
Affected Version(s): 2016					
N/A	09-Aug-2022	7.3	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-33631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33631	A-MIC-EXCE-170822/1130
Product: exchange_server					
Affected Version(s): 2013					
N/A	09-Aug-2022	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21980, CVE-2022-24477. **CVE ID : CVE-2022-24516**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24516	A-MIC-EXCH-170822/1131
N/A	09-Aug-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24477, CVE-2022-24516. **CVE ID : CVE-2022-21980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21980	A-MIC-EXCH-170822/1132
N/A	09-Aug-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-EXCH-170822/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-21980, CVE-2022-24516. **CVE ID : CVE-2022-24477**	guidance/advisory/CVE-2022-24477	
N/A	09-Aug-2022	6.5	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30134, CVE-2022-34692. **CVE ID : CVE-2022-21979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21979	A-MIC-EXCH-170822/1134
N/A	09-Aug-2022	5.3	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21979, CVE-2022-34692. **CVE ID : CVE-2022-30134**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30134	A-MIC-EXCH-170822/1135
Affected Version(s): 2016					
N/A	09-Aug-2022	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21980, CVE-2022-24477. **CVE ID : CVE-2022-24516**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24516	A-MIC-EXCH-170822/1136
N/A	09-Aug-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	A-MIC-EXCH-170822/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-24477, CVE-2022-24516. **CVE ID : CVE-2022-21980**	guidance/advisory/CVE-2022-21980	
N/A	09-Aug-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21980, CVE-2022-24516. **CVE ID : CVE-2022-24477**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24477	A-MIC-EXCH-170822/1138
N/A	09-Aug-2022	6.5	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30134, CVE-2022-34692. **CVE ID : CVE-2022-21979**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21979	A-MIC-EXCH-170822/1139
N/A	09-Aug-2022	5.3	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21979, CVE-2022-34692. **CVE ID : CVE-2022-30134**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30134	A-MIC-EXCH-170822/1140
N/A	09-Aug-2022	5.3	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-EXCH-170822/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-21979, CVE-2022-30134. **CVE ID : CVE-2022-34692**	ory/CVE-2022-34692	
Affected Version(s): 2019					
N/A	09-Aug-2022	9.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21980, CVE-2022-24477. **CVE ID : CVE-2022-24516**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24516	A-MIC-EXCH-170822/1142
N/A	09-Aug-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24477, CVE-2022-24516. **CVE ID : CVE-2022-21980**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21980	A-MIC-EXCH-170822/1143
N/A	09-Aug-2022	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21980, CVE-2022-24516. **CVE ID : CVE-2022-24477**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24477	A-MIC-EXCH-170822/1144
N/A	09-Aug-2022	6.5	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-EXCH-170822/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-30134, CVE-2022-34692. **CVE ID : CVE-2022-21979**	ory/CVE-2022-21979	
N/A	09-Aug-2022	5.3	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21979, CVE-2022-34692. **CVE ID : CVE-2022-30134**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30134	A-MIC-EXCH-170822/1146
N/A	09-Aug-2022	5.3	Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21979, CVE-2022-30134. **CVE ID : CVE-2022-34692**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34692	A-MIC-EXCH-170822/1147
Product: microsoft_advertising_universal_event_tracking					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	4.8	The Microsoft Advertising Universal Event Tracking (UET) WordPress plugin before 1.0.4 does not sanitise and escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html	N/A	A-MIC-MICR-170822/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability is disallowed. Due to the nature of this plugin, well crafted XSS can also leak into the frontpage. **CVE ID : CVE-2022-2170**		
Product: office					
Affected Version(s): 2013					
N/A	09-Aug-2022	8.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34717	A-MIC-OFFI-170822/1149
Affected Version(s): 2016					
N/A	09-Aug-2022	8.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34717	A-MIC-OFFI-170822/1150
Affected Version(s): 2019					
N/A	09-Aug-2022	8.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34717	A-MIC-OFFI-170822/1151
N/A	09-Aug-2022	7.3	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-33631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33631	A-MIC-OFFI-170822/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: office_long_term_servicing_channel					
Affected Version(s): 2021					
N/A	09-Aug-2022	8.8	Microsoft Office Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34717**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34717	A-MIC-OFFI-170822/1153
N/A	09-Aug-2022	7.3	Microsoft Excel Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-33631**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33631	A-MIC-OFFI-170822/1154
Product: office_online_server					
Affected Version(s): -					
N/A	09-Aug-2022	7.8	Microsoft Excel Remote Code Execution Vulnerability. **CVE ID : CVE-2022-33648**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33648	A-MIC-OFFI-170822/1155
Product: open_management_infrastructure					
Affected Version(s): * Up to (excluding) 1.6.10-2					
N/A	09-Aug-2022	7.8	System Center Operations Manager: Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-33640**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33640	A-MIC-OPEN-170822/1156
Product: powershell					
Affected Version(s): From (including) 7.0 Up to (excluding) 7.0.12					
N/A	09-Aug-2022	5.9	.NET Spoofing Vulnerability.	https://portal.msrc.microsoft.	A-MIC-POWE-170822/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34716	com/en-US/security-guidance/advisory/CVE-2022-34716	
Affected Version(s): From (including) 7.2 Up to (excluding) 7.2.6					
N/A	09-Aug-2022	5.9	.NET Spoofing Vulnerability. **CVE ID : CVE-2022-34716**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34716	A-MIC-POWE-170822/1158
Product: system_center_operations_manager					
Affected Version(s): 2016					
N/A	09-Aug-2022	7.8	System Center Operations Manager: Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-33640**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33640	A-MIC-SYST-170822/1159
Affected Version(s): 2019					
N/A	09-Aug-2022	7.8	System Center Operations Manager: Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-33640**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33640	A-MIC-SYST-170822/1160
Affected Version(s): 2022					
N/A	09-Aug-2022	7.8	System Center Operations Manager: Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33640	A-MIC-SYST-170822/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33640		
Product: visual_studio					
Affected Version(s): 2013					
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35825, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35777**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35777	A-MIC-VISU-170822/1162
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1163
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1164
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35827	A-MIC-VISU-170822/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35825, CVE-2022-35826. **CVE ID : CVE-2022-35827**		
Affected Version(s): 2012					
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35825, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35777**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35777	A-MIC-VISU-170822/1166
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1167
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1168
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-VISU-170822/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35825, CVE-2022-35826. **CVE ID : CVE-2022-35827**	ory/CVE-2022-35827	
Affected Version(s): 2015					
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35825, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35777**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35777	A-MIC-VISU-170822/1170
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1171
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1172
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	A-MIC-VISU-170822/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35825, CVE-2022-35826. **CVE ID : CVE-2022-35827**	ory/CVE-2022-35827	
Product: visual_studio_2017					
Affected Version(s): 15.9					
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1174
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1175
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35826. **CVE ID : CVE-2022-35827**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35827	A-MIC-VISU-170822/1176
Affected Version(s): From (including) 15.0 Up to (including) 15.9					
Improper Control of Generation	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-	A-MIC-VISU-170822/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			CVE ID is unique from CVE-2022-35825, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35777**	US/security-guidance/advisory/CVE-2022-35777	
Product: visual_studio_2019					
Affected Version(s): 16.11					
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1178
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1179
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35826. **CVE ID : CVE-2022-35827**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35827	A-MIC-VISU-170822/1180
Affected Version(s): 16.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1181
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1182
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35826. **CVE ID : CVE-2022-35827**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35827	A-MIC-VISU-170822/1183
Affected Version(s): From (including) 16.0 Up to (including) 16.11					
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35825, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35777**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35777	A-MIC-VISU-170822/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: visual_studio_2022					
Affected Version(s): 17.0					
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35825, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35777**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35777	A-MIC-VISU-170822/1185
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1186
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1187
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35826.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35827	A-MIC-VISU-170822/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35827		
Affected Version(s): 17.2					
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35825, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35777**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35777	A-MIC-VISU-170822/1189
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35826, CVE-2022-35827. **CVE ID : CVE-2022-35825**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825	A-MIC-VISU-170822/1190
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35827. **CVE ID : CVE-2022-35826**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35826	A-MIC-VISU-170822/1191
N/A	09-Aug-2022	8.8	Visual Studio Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35777, CVE-2022-35825, CVE-2022-35826.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35827	A-MIC-VISU-170822/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35827		
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.1. **CVE ID : CVE-2022-2777**	https://github.com/microweber/microweber/commit/60eef7494211d1c458228c321e986edeaa401a58, https://huntr.dev/bounties/13dd2f4d-0c7f-483e-a771-e1ed2ff1c36f	A-MIC-MICR-170822/1193
Vendor: milkytracker_project					
Product: milkytracker					
Affected Version(s): 1.03.00					
Out-of-bounds Write	03-Aug-2022	7.8	MilkyTracker v1.03.00 was discovered to contain a stack overflow via the component LoaderXM::load. This vulnerability is triggered when the program is supplied a crafted XM module file. **CVE ID : CVE-2022-34927**	https://github.com/milkytracker/MilkyTracker/commit/3a5474f9102cbdc10fbd9e7b1b2c8d3f3f45d91b, https://github.com/milkytracker/MilkyTracker/issues/275	A-MIL-MILK-170822/1194
Vendor: minio					
Product: minio					
Affected Version(s): * Up to (excluding) 2022-07-29t19-40-48z					
Improper Limitation	01-Aug-2022	2.7	MinIO is a High Performance Object	https://github.com/minio/mi	A-MIN-MINI-170822/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Storage released under GNU Affero General Public License v3.0. In affected versions all 'admin' users authorized for `admin:ServerUpdate` can selectively trigger an error that in response, returns the content of the path requested. Any normal OS system would allow access to contents at any arbitrary paths that are readable by MinIO process. Users are advised to upgrade. Users unable to upgrade may disable ServerUpdate API by denying the `admin:ServerUpdate` action for your admin users via IAM policies. **CVE ID : CVE-2022-35919**	nio/commit/bc72e4226e669d98c8e0f3eccc9297be9251c692, https://github.com/minio/minio/pull/15429, https://github.com/minio/minio/security/advisories/GHSA-gr9v-6pcm-rqvg	
Vendor: monetdb					
Product: monetdb					
Affected Version(s): 11.43.13					
Reachable Assertion	03-Aug-2022	7.5	The assertion `stmt->Dbc->FirstStmt' failed in MonetDB Database Server v11.43.13. **CVE ID : CVE-2022-34967**	https://github.com/MonetDB/MonetDB/issues/7306	A-MON-MONE-170822/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: mtouch_quiz_project					
Product: mtouch_quiz					
Affected Version(s): * Up to (including) 3.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The mTouch Quiz WordPress plugin through 3.1.3 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 when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2410**	N/A	A-MTO-MTOU-170822/1197
Vendor: multi_language_hotel_management_software_project					
Product: multi_language_hotel_management_software					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2022	9.8	A vulnerability was found in SourceCodester Multi Language Hotel Management Software. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument room_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may	N/A	A-MUL-MULT-170822/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The associated identifier of this vulnerability is VDB-205595. **CVE ID : CVE-2022-2648**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2022	9.8	A vulnerability classified as critical has been found in SourceCodester Multi Language Hotel Management Software. Affected is an unknown function. The manipulation of the argument email 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-205596. **CVE ID : CVE-2022-2656**	N/A	A-MUL-MULT-170822/1199
Vendor: Najeebmedia					
Product: wordpress_comments_fields					
Affected Version(s): * Up to (excluding) 4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The WordPress Comments Fields WordPress plugin before 4.1 does not escape Field Error Message, which could allow high-privileged users to perform Cross-Site Scripting attacks	N/A	A-NAJ-WORD-170822/1200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even when unfiltered_html is disallowed **CVE ID : CVE-2022-2398**		
Vendor: Netapp					
Product: storagegrid					
Affected Version(s): From (including) 11.6.0 Up to (excluding) 11.6.0.3					
N/A	10-Aug-2022	6.5	Linux deployments of StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.2 deployed with a Linux kernel version less than 4.7.0 are susceptible to a vulnerability which could allow a remote unauthenticated attacker to view limited metrics information and modify alert email recipients and content. **CVE ID : CVE-2022-23238**	https://security.netapp.com/advisory/NTAP-20220808-0001/	A-NET-STOR-170822/1201
Vendor: next-auth					
Product: nextauth.js					
Affected Version(s): * Up to (excluding) 3.29.9					
Insertion of Sensitive Information into Log File	01-Aug-2022	3.3	NextAuth.js is a complete open source authentication solution for Next.js applications. An information disclosure	https://next-auth.js.org/getting-started/upgrade-v4, https://next-auth.js.org/warnings#debug_e	A-NEX-NEXT-170822/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in `next-auth` before `v4.10.2` and `v3.29.9` allows an attacker with log access privilege to obtain excessive information such as an identity provider's secret in the log (which is thrown during OAuth error handling) and use it to leverage further attacks on the system, like impersonating the client to ask for extensive permissions. This issue has been patched in `v4.10.2` and `v3.29.9` by moving the log for `provider` information to the debug level. In addition, we added a warning for having the `debug: true` option turned on in production. If for some reason you cannot upgrade, you can user the `logger` configuration option by sanitizing the logs. **CVE ID : CVE-2022-31186**	nabled, https://github.com/nextauthjs/next-auth/security/advisories/GHSA-p6mm-27gq-9v3p, https://next-auth.js.org/configuration/options#logger	
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.10.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	01-Aug-2022	3.3	NextAuth.js is a complete open source authentication solution for Next.js applications. An information disclosure vulnerability in `next-auth` before `v4.10.2` and `v3.29.9` allows an attacker with log access privilege to obtain excessive information such as an identity provider's secret in the log (which is thrown during OAuth error handling) and use it to leverage further attacks on the system, like impersonating the client to ask for extensive permissions. This issue has been patched in `v4.10.2` and `v3.29.9` by moving the log for `provider` information to the debug level. In addition, we added a warning for having the `debug: true` option turned on in production. If for some reason you cannot upgrade, you can user the `logger`	https://next-auth.js.org/getting-started/upgrade-v4, https://next-auth.js.org/warnings#debug_enabled, https://github.com/nextauthjs/next-auth/security/advisories/GHSA-p6mm-27gq-9v3p, https://next-auth.js.org/configuration/options#logger	A-NEX-NEXT-170822/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration option by sanitizing the logs. **CVE ID : CVE-2022-31186**		
Vendor: nextauth.js					
Product: next-auth					
Affected Version(s): * Up to (excluding) 3.29.10					
Incorrect Authorization	02-Aug-2022	9.1	NextAuth.js is a complete open source authentication solution for Next.js applications. `next-auth` users who are using the `EmailProvider` either in versions before `4.10.3` or `3.29.10` are affected. If an attacker could forge a request that sent a comma-separated list of emails (eg.: `attacker@attacker.com,victim@victim.com`) to the sign-in endpoint, NextAuth.js would send emails to both the attacker and the victim's e-mail addresses. The attacker could then login as a newly created user with the email being `attacker@attacker.com,victim@victim.com`. This means that basic authorization	https://next-auth.js.org/configuration/callbacks#sign-in-callback, https://github.com/nextauthjs/next-auth/security/advisories/GHSA-xv97-c62v-4587, https://next-auth.js.org/providers/email#normalizing-the-e-mail-address	A-NEX-NEXT-170822/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			like `email.endsWith("@victim.com")` in the `signIn` callback would fail to communicate a threat to the developer and would let the attacker bypass authorization, even with an `@attacker.com` address. This vulnerability has been patched in `v4.10.3` and `v3.29.10` by normalizing the email value that is sent to the sign-in endpoint before accessing it anywhere else. We also added a `normalizeIdentifier` callback on the `EmailProvider` configuration, where you can further tweak your requirements for what your system considers a valid e-mail address. (E.g.: strict RFC2821 compliance). Users are advised to upgrade. There are no known workarounds for this vulnerability. If for some reason you cannot upgrade, you		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can normalize the incoming request using Advanced Initialization. **CVE ID : CVE-2022-35924**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.10.3					
Incorrect Authorization	02-Aug-2022	9.1	NextAuth.js is a complete open source authentication solution for Next.js applications. `next-auth` users who are using the `EmailProvider` either in versions before `4.10.3` or `3.29.10` are affected. If an attacker could forge a request that sent a comma-separated list of emails (eg.: `attacker@attacker.com,victim@victim.com`) to the sign-in endpoint, NextAuth.js would send emails to both the attacker and the victim's e-mail addresses. The attacker could then login as a newly created user with the email being `attacker@attacker.com,victim@victim.com`. This means that basic authorization like `email.endsWith("@v	https://next-auth.js.org/configuration/callbacks#sign-in-callback, https://github.com/nextauthjs/next-auth/security/advisories/GHSA-xv97-c62v-4587, https://next-auth.js.org/providers/email#normalizing-the-e-mail-address	A-NEX-NEXT-170822/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ictim.com")` in the `signIn` callback would fail to communicate a threat to the developer and would let the attacker bypass authorization, even with an `@attacker.com` address. This vulnerability has been patched in `v4.10.3` and `v3.29.10` by normalizing the email value that is sent to the sign-in endpoint before accessing it anywhere else. We also added a `normalizeIdentifier` callback on the `EmailProvider` configuration, where you can further tweak your requirements for what your system considers a valid e-mail address. (E.g.: strict RFC2821 compliance). Users are advised to upgrade. There are no known workarounds for this vulnerability. If for some reason you cannot upgrade, you can normalize the incoming request		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using Advanced Initialization. **CVE ID : CVE-2022-35924**		
Vendor: Nextcloud					
Product: mail					
Affected Version(s): * Up to (excluding) 1.12.1					
Insertion of Sensitive Information into Log File	04-Aug-2022	4.9	Nextcloud Mail is an email application for the nextcloud personal cloud product. Affected versions of Nextcloud mail would log user passwords to disk in the event of a misconfiguration. Should an attacker gain access to the logs complete access to affected accounts would be obtainable. It is recommended that the Nextcloud Mail is upgraded to 1.12.1. Operators should inspect their logs and remove passwords which have been logged. There are no workarounds to prevent logging in the event of a misconfiguration. **CVE ID : CVE-2022-31119**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-63m3-w68h-3wjg, https://github.com/nextcloud/mail/pull/6488/commits/ab9ade57fbc1f465ffe905248f93f328d638d7e5	A-NEX-MAIL-170822/1206
Affected Version(s): * Up to (excluding) 1.12.8					
Server-Side	04-Aug-2022	9.8	Nextcloud Mail is an email application for	https://github.com/nextcloud	A-NEX-MAIL-170822/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			the nextcloud personal cloud product. Affected versions shipped with a CSS minifier on the path `./vendor/cerdic/css-tidy/css_optimiser.php`. Access to the minifier is unrestricted and access may lead to Server-Side Request Forgery (SSRF). It is recommendet to upgrade to Mail 1.12.7 or Mail 1.13.6. Users unable to upgrade may manually delete the file located at `./vendor/cerdic/css-tidy/css_optimiser.php` **CVE ID : CVE-2022-31132**	/security-advisories/security/advisories/GHSA-24pm-rjfv-23mh	
Affected Version(s): From (including) 1.13.0 Up to (excluding) 1.13.6					
Server-Side Request Forgery (SSRF)	04-Aug-2022	9.8	Nextcloud Mail is an email application for the nextcloud personal cloud product. Affected versions shipped with a CSS minifier on the path `./vendor/cerdic/css-tidy/css_optimiser.php`. Access to the minifier is unrestricted and	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-24pm-rjfv-23mh	A-NEX-MAIL-170822/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access may lead to Server-Side Request Forgery (SSRF). It is recommendet to upgrade to Mail 1.12.7 or Mail 1.13.6. Users unable to upgrade may manually delete the file located at `./vendor/cerdic/css-tidy/css_optimiser.php` **CVE ID : CVE-2022-31132**		
Product: nextcloud_server					
Affected Version(s): * Up to (excluding) 22.2.7					
N/A	04-Aug-2022	2.7	Nextcloud server is an open source personal cloud solution. The audit log is used to get a full trail of the actions which has been incompletely populated. In affected versions federated share events were not properly logged which would allow brute force attacks to go unnoticed. This behavior exacerbates the impact of CVE-2022-31118. It is recommended that the Nextcloud Server is upgraded to 22.2.7, 23.0.4 or 24.0.0. There are no	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-9qvg-7fwg-722x, https://github.com/nextcloud/server/pull/31594/commits/1d8bf9a89c6856218802a1d365000a5831be8655, https://portal.nextcloud.com/article/using-the-audit-log-44.html	A-NEX-NEXT-170822/1209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds available. **CVE ID : CVE-2022-31120**		
Affected Version(s): * Up to (excluding) 22.2.9					
Improper Restriction of Excessive Authentication Attempts	04-Aug-2022	5.3	Nextcloud server is an open source personal cloud solution. In affected versions an attacker could brute force to find if federated sharing is being used and potentially try to brute force access tokens for federated shares (`a-zA-Z0-9` ^ 15). It is recommended that the Nextcloud Server is upgraded to 22.2.9, 23.0.6 or 24.0.2. Users unable to upgrade may disable federated sharing via the Admin Sharing settings in `index.php/settings/admin/sharing`. **CVE ID : CVE-2022-31118**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-2vwh-5v93-3vcq, https://github.com/nextcloud/server/pull/32843/commits/6eb692da7fe73c899cb6a8d2aa045eddb1f14018	A-NEX-NEXT-170822/1210
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.4					
N/A	04-Aug-2022	2.7	Nextcloud server is an open source personal cloud solution. The audit log is used to get a full trail of the actions which has been incompletely populated. In	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-9qvg-7fwg-722x, https://github.com/nextcloud	A-NEX-NEXT-170822/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected versions federated share events were not properly logged which would allow brute force attacks to go unnoticed. This behavior exacerbates the impact of CVE-2022-31118. It is recommended that the Nextcloud Server is upgraded to 22.2.7, 23.0.4 or 24.0.0. There are no workarounds available. **CVE ID : CVE-2022-31120**	/server/pull/31594/commits/1d8bf9a89c6856218802a1d365000a5831be8655, https://portal.nextcloud.com/article/using-the-audit-log-44.html	
Affected Version(s): From (including) 23.0.0 Up to (excluding) 23.0.6					
Improper Restriction of Excessive Authentication Attempts	04-Aug-2022	5.3	Nextcloud server is an open source personal cloud solution. In affected versions an attacker could brute force to find if federated sharing is being used and potentially try to brute force access tokens for federated shares (`a-zA-Z0-9` ^ 15). It is recommended that the Nextcloud Server is upgraded to 22.2.9, 23.0.6 or 24.0.2. Users unable to upgrade may disable federated sharing via the Admin Sharing settings in	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-2vwh-5v93-3vcq, https://github.com/nextcloud/server/pull/32843/commits/6eb692da7fe73c899cb6a8d2aa045eddb1f14018	A-NEX-NEXT-170822/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`index.php/settings/admin/sharing`. **CVE ID : CVE-2022-31118**		
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.0.2					
Improper Restriction of Excessive Authentication Attempts	04-Aug-2022	5.3	Nextcloud server is an open source personal cloud solution. In affected versions an attacker could brute force to find if federated sharing is being used and potentially try to brute force access tokens for federated shares (`a-zA-Z0-9` ^ 15). It is recommended that the Nextcloud Server is upgraded to 22.2.9, 23.0.6 or 24.0.2. Users unable to upgrade may disable federated sharing via the Admin Sharing settings in `index.php/settings/admin/sharing`. **CVE ID : CVE-2022-31118**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-2vwh-5v93-3vcq, https://github.com/nextcloud/server/pull/32843/commits/6eb692da7fe73c899cb6a8d2aa045eddb1f14018	A-NEX-NEXT-170822/1213
Product: talk					
Affected Version(s): * Up to (excluding) 12.2.7					
Improper Restriction of Excessive Authentication Attempts	12-Aug-2022	5.3	Nextcloud Talk is a video and audio conferencing app for Nextcloud. Prior to versions 12.2.7, 13.0.7, and 14.0.3, password protected conversations are	https://github.com/nextcloud/spreed/pull/7536, https://github.com/nextcloud/spreed/commit/04300bbed0	A-NEX-TALK-170822/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			susceptible to brute force attacks if the attacker has the link/conversation token. It is recommended that the Nextcloud Talk application is upgraded to 12.2.7, 13.0.7 or 14.0.3. There are currently no known workarounds available apart from not having password protected conversations. **CVE ID : CVE-2022-35932**	e87ff3420b5d752bbc48e2c15f35e9, https://github.com/nextcloud/spreed/pull/7535, https://github.com/nextcloud/spreed/pull/7504	
Affected Version(s): From (including) 13.0.0 Up to (excluding) 13.0.7					
Improper Restriction of Excessive Authentication Attempts	12-Aug-2022	5.3	Nextcloud Talk is a video and audio conferencing app for Nextcloud. Prior to versions 12.2.7, 13.0.7, and 14.0.3, password protected conversations are susceptible to brute force attacks if the attacker has the link/conversation token. It is recommended that the Nextcloud Talk application is upgraded to 12.2.7, 13.0.7 or 14.0.3. There are currently no known workarounds available apart from not having password	https://github.com/nextcloud/spreed/pull/7536, https://github.com/nextcloud/spreed/commit/04300bbed0e87ff3420b5d752bbc48e2c15f35e9, https://github.com/nextcloud/spreed/pull/7535, https://github.com/nextcloud/spreed/pull/7504	A-NEX-TALK-170822/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protected conversations. **CVE ID : CVE-2022-35932**		
Affected Version(s): From (including) 14.0.0 Up to (excluding) 14.0.3					
Improper Restriction of Excessive Authentication Attempts	12-Aug-2022	5.3	Nextcloud Talk is a video and audio conferencing app for Nextcloud. Prior to versions 12.2.7, 13.0.7, and 14.0.3, password protected conversations are susceptible to brute force attacks if the attacker has the link/conversation token. It is recommended that the Nextcloud Talk application is upgraded to 12.2.7, 13.0.7 or 14.0.3. There are currently no known workarounds available apart from not having password protected conversations. **CVE ID : CVE-2022-35932**	https://github.com/nextcloud/spreed/pull/7536, https://github.com/nextcloud/spreed/commit/04300bbed0e87ff3420b5d752bbc48e2c15f35e9, https://github.com/nextcloud/spreed/pull/7535, https://github.com/nextcloud/spreed/pull/7504	A-NEX-TALK-170822/1216
Vendor: nhi					
Product: health_insurance_web_service_component					
Affected Version(s): -					
Out-of-bounds Write	02-Aug-2022	7.8	The NHI card's web service component has a stack-based buffer overflow vulnerability due to insufficient	N/A	A-NHI-HEAL-170822/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation for network packet header length. A local area network attacker with general user privilege can exploit this vulnerability to execute arbitrary code, manipulate system command or disrupt service. **CVE ID : CVE-2022-35217**		
Allocation of Resources Without Limits or Throttling	02-Aug-2022	5.5	The NHI card's web service component has a heap-based buffer overflow vulnerability due to insufficient validation for packet origin parameter length. A LAN attacker with general user privilege can exploit this vulnerability to disrupt service. **CVE ID : CVE-2022-35218**	N/A	A-NHI-HEAL-170822/1218
Allocation of Resources Without Limits or Throttling	02-Aug-2022	5.5	The NHI card's web service component has a stack-based buffer overflow vulnerability due to insufficient validation for network packet key parameter. A LAN attacker with general user privilege can exploit this	N/A	A-NHI-HEAL-170822/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to disrupt service. **CVE ID : CVE-2022-35219**		
Vendor: Nlnetlabs					
Product: unbound					
Affected Version(s): * Up to (excluding) 1.16.2					
Insufficient Session Expiration	01-Aug-2022	6.5	NLnet Labs Unbound, up to and including version 1.16.1 is vulnerable to a novel type of the "ghost domain names" attack. The vulnerability works by targeting an Unbound instance. Unbound is queried for a subdomain of a rogue domain name. The rogue nameserver returns delegation information for the subdomain that updates Unbound's delegation cache. This action can be repeated before expiry of the delegation information by querying Unbound for a second level subdomain which the rogue nameserver provides new delegation information. Since Unbound is a child-centric resolver, the ever-updating child	https://www.nlnetlabs.nl/downloads/unbound/CVE-2022-30698_CVE-2022-30699.txt	A-NLN-UNBO-170822/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delegation information can keep a rogue domain name resolvable long after revocation. From version 1.16.2 on, Unbound checks the validity of parent delegation records before using cached delegation information. **CVE ID : CVE-2022-30698**		
Insufficient Session Expiration	01-Aug-2022	6.5	NLnet Labs Unbound, up to and including version 1.16.1, is vulnerable to a novel type of the "ghost domain names" attack. The vulnerability works by targeting an Unbound instance. Unbound is queried for a rogue domain name when the cached delegation information is about to expire. The rogue nameserver delays the response so that the cached delegation information is expired. Upon receiving the delayed answer containing the delegation information, Unbound overwrites the now expired entries. This action	https://www.nlnetlabs.nl/downloads/unbound/CVE-2022-30698_CVE-2022-30699.txt	A-NLN-UNBO-170822/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can be repeated when the delegation information is about to expire making the rogue delegation information ever-updating. From version 1.16.2 on, Unbound stores the start time for a query and uses that to decide if the cached delegation information can be overwritten. **CVE ID : CVE-2022-30699**		
Vendor: node-fetch_project					
Product: node-fetch					
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.2.10					
Uncontrolled Resource Consumption	01-Aug-2022	5.9	Denial of Service in GitHub repository node-fetch/node-fetch prior to 3.2.10. **CVE ID : CVE-2022-2596**	https://github.com/node-fetch/node-fetch/commit/28802387292baee467e042e168d92597b5bbbe3d, https://huntr.dev/bounties/a7e6a136-0a4b-46c4-ad20-802f1dd60bf7	A-NOD-NODE-170822/1222
Vendor: Nvidia					
Product: virtual_gpu					
Affected Version(s): 14.0					
Incorrect Authorization	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin),	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where it allows the guest VM to allocate resources for which the guest is not authorized. This vulnerability may lead to loss of data integrity and confidentiality, denial of service, or information disclosure. **CVE ID : CVE-2022-31609**		
Double Free	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin) where it may double-free some resources. An attacker may exploit this vulnerability with other vulnerabilities to cause denial of service, code execution, and information disclosure. **CVE ID : CVE-2022-31614**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1224
NULL Pointer Dereference	05-Aug-2022	5.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a null pointer, which may lead to denial of service.	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31618		
Affected Version(s): 14.1					
Incorrect Authorization	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it allows the guest VM to allocate resources for which the guest is not authorized. This vulnerability may lead to loss of data integrity and confidentiality, denial of service, or information disclosure. **CVE ID : CVE-2022-31609**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1226
Double Free	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin) where it may double-free some resources. An attacker may exploit this vulnerability with other vulnerabilities to cause denial of service, code execution, and information disclosure. **CVE ID : CVE-2022-31614**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1227
NULL Pointer	05-Aug-2022	5.5	NVIDIA vGPU software contains a	https://nvidia.custhelp.com/ap	A-NVI-VIRT-170822/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a null pointer, which may lead to denial of service. **CVE ID : CVE-2022-31618**	p/answers/det ail/a_id/5383	
Affected Version(s): From (including) 11.0 Up to (excluding) 11.8					
Incorrect Authorizati on	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it allows the guest VM to allocate resources for which the guest is not authorized. This vulnerability may lead to loss of data integrity and confidentiality, denial of service, or information disclosure. **CVE ID : CVE-2022-31609**	https://nvidia.c usthelp.com/ap p/answers/det ail/a_id/5383	A-NVI-VIRT-170822/1229
Double Free	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin) where it may double-free some resources. An attacker may exploit this vulnerability with other vulnerabilities to cause denial of	https://nvidia.c usthelp.com/ap p/answers/det ail/a_id/5383	A-NVI-VIRT-170822/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service, code execution, and information disclosure. **CVE ID : CVE-2022-31614**		
NULL Pointer Dereference	05-Aug-2022	5.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a null pointer, which may lead to denial of service. **CVE ID : CVE-2022-31618**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1231
Affected Version(s): From (including) 13.0 Up to (excluding) 13.3					
Incorrect Authorization	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it allows the guest VM to allocate resources for which the guest is not authorized. This vulnerability may lead to loss of data integrity and confidentiality, denial of service, or information disclosure. **CVE ID : CVE-2022-31609**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1232
Double Free	05-Aug-2022	7.8	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager	https://nvidia.custhelp.com/ap	A-NVI-VIRT-170822/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(vGPU plugin) where it may double-free some resources. An attacker may exploit this vulnerability with other vulnerabilities to cause denial of service, code execution, and information disclosure. **CVE ID : CVE-2022-31614**	p/answers/detail/a_id/5383	
NULL Pointer Dereference	05-Aug-2022	5.5	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a null pointer, which may lead to denial of service. **CVE ID : CVE-2022-31618**	https://nvidia.custhelp.com/app/answers/detail/a_id/5383	A-NVI-VIRT-170822/1234
Vendor: omicard_edm_project					
Product: omicard_edm					
Affected Version(s): From (including) 5.8 Up to (including) 6.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2022	9.8	OMICARD EDM's API function has insufficient validation for user input. An unauthenticated remote attacker can inject arbitrary SQL commands to access, modify, delete database or disrupt service.	N/A	A-OMI-OMIC-170822/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-32964		
Use of Hard-coded Credentials	04-Aug-2022	9.8	OMICARD EDM has a hard-coded machine key. An unauthenticated remote attacker can use the machine key to send serialized payload to the server to execute arbitrary code, manipulate system data and disrupt service. **CVE ID : CVE-2022-32965**	N/A	A-OMI-OMIC-170822/1236
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	OMICARD EDM's mail file relay function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to by-pass authentication and access arbitrary system files. **CVE ID : CVE-2022-32963**	N/A	A-OMI-OMIC-170822/1237
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	OMICARD EDM's mail image relay function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to by-pass authentication and access arbitrary system files.	N/A	A-OMI-OMIC-170822/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35216		
Vendor: online_admission_system_project					
Product: online_admission_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2022	9.8	A vulnerability has been found in SourceCodester Online Admission System and classified as critical. This vulnerability affects unknown code of the component POST Parameter Handler. The manipulation of the argument shift 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 entry is VDB-205564. **CVE ID : CVE-2022-2643**	N/A	A-ONL-ONLI-170822/1239
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Aug-2022	9.8	A vulnerability was found in SourceCodester Online Admission System and classified as critical. This issue affects some unknown processing of the component GET Parameter Handler. The manipulation of the argument eid leads to sql injection. The	N/A	A-ONL-ONLI-170822/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The identifier VDB-205565 was assigned to this vulnerability. **CVE ID : CVE-2022-2644**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2022	6.1	A vulnerability, which was classified as problematic, was found in SourceCodester Online Admission System. Affected is an unknown function of the file index.php. The manipulation of the argument eid with the input 8</h3><script>alert (1)</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-205572. **CVE ID : CVE-2022-2646**	N/A	A-ONL-ONLI-170822/1241
Improper Neutralization of Input During Web Page Generation	11-Aug-2022	6.1	A vulnerability classified as problematic has been found in SourceCodester Online Admission System. This affects an unknown part of the file /index.php.	N/A	A-ONL-ONLI-170822/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			The manipulation of the argument student_add 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-206163. **CVE ID : CVE-2022-2767**		
Vendor: online_class_and_exam_scheduling_system_project					
Product: online_class_and_exam_scheduling_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	9.8	A vulnerability classified as critical has been found in SourceCodester Online Class and Exam Scheduling System 1.0. Affected is an unknown function of the file /pages/class_sched.php. The manipulation of the argument class with the input '||(SELECT 0x684d6b6c WHERE 5993=5993 AND (SELECT 2096 FROM(SELECT COUNT(*),CONCAT(0x717a786b71,(SELECT (ELT(2096=2096,1))),0x717a626271,FLOOR(RAND(0)*2))x	N/A	A-ONL-ONLI-170822/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||' 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-205830 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2706**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	9.8	A vulnerability classified as critical was found in SourceCodester Online Class and Exam Scheduling System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/faculty_sched.php. The manipulation of the argument faculty with the input ' OR (SELECT 2078 FROM(SELECT COUNT(*),CONCAT(0x716a717071,(SELECT (ELT(2078=2078,1))),0x717a706a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS	N/A	A-ONL-ONLI-170822/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GROUP BY x)a)--uYCM 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-205831. **CVE ID : CVE-2022-2707**		
Vendor: online_student_admission_system_project					
Product: online_student_admission_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	A vulnerability classified as problematic was found in SourceCodester Online Student Admission System. Affected by this vulnerability is an unknown functionality of the file edit-profile.php of the component Student User Page. The manipulation with the input <script>alert(/xss/)</script> leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205669 was	N/A	A-ONL-ONLI-170822/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2022-2681**		
Vendor: online_tours_and_travels_management_system_project					
Product: online_tours_and_travels_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	7.2	Online Tours And Travels Management System v1.0 was discovered to contain a SQL injection vulnerability via the pname parameter at /admin/operations/packages.php. **CVE ID : CVE-2022-35421**	N/A	A-ONL-ONLI-170822/1246
Vendor: Open-emr					
Product: openemr					
Affected Version(s): * Up to (excluding) 7.0.0.1					
Improper Privilege Management	09-Aug-2022	8.3	Improper Privilege Management in GitHub repository openemr/openemr prior to 7.0.0.1. **CVE ID : CVE-2022-2732**	https://github.com/openemr/openemr/commit/2973592bc7b1f4996738a6fd27d1e277e33676b6, https://huntr.dev/bounties/8773e0d1-5f1a-4e87-8998-f5ec45f6d533	A-OPE-OPEN-170822/1247
Authorization Bypass Through User-Controlled Key	09-Aug-2022	6.5	Authorization Bypass Through User-Controlled Key in GitHub repository openemr/openemr prior to 7.0.0.1.	https://github.com/openemr/openemr/commit/2973592bc7b1f4996738a6fd27d1e277e	A-OPE-OPEN-170822/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2730	33676b6, https://huntr.dev/bounties/a81f39ab-092b-4941-b9ca-c4c8f2191504	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1. **CVE ID : CVE-2022-2731**	https://huntr.dev/bounties/20b8d5c5-0764-4f0b-8ab3-b9f6b857175e, https://github.com/openemr/openemr/commit/285fb234bd27ea4c46a29f2797edda7f38f1d8db	A-OPE-OPEN-170822/1249
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1. **CVE ID : CVE-2022-2733**	https://huntr.dev/bounties/25b91301-dfb0-4353-a732-e051bbe8420c, https://github.com/openemr/openemr/commit/59458bc15ab0cb556c521de9d5187167d6f88945	A-OPE-OPEN-170822/1250
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-2022	5.4	Cross-site Scripting (XSS) - DOM in GitHub repository openemr/openemr prior to 7.0.0.1. **CVE ID : CVE-2022-2729**	https://huntr.dev/bounties/13b58e74-2dd0-4eec-9f3a-554485701540, https://github.com/openemr/openemr/commit/74d21039aec641b2c406e3baf238ae4602a968b6	A-OPE-OPEN-170822/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	09-Aug-2022	5.4	Improper Restriction of Rendered UI Layers or Frames in GitHub repository openemr/openemr prior to 7.0.0.1. **CVE ID : CVE-2022-2734**	https://huntr.dev/bounties/d8e4c70c-788b-47e9-8141-a08db751d4e6, https://github.com/openemr/openemr/commit/203243467675e85b8b479c778e44ae1aac8bad55	A-OPE-OPEN-170822/1252
Vendor: Openstack					
Product: nova					
Affected Version(s): * Up to (excluding) 23.2.2					
N/A	03-Aug-2022	3.3	An issue was discovered in OpenStack Nova before 23.2.2, 24.x before 24.1.2, and 25.x before 25.0.2. By creating a neutron port with the direct vnic_type, creating an instance bound to that port, and then changing the vnic_type of the bound port to macvtap, an authenticated user may cause the compute service to fail to restart, resulting in a possible denial of service. Only Nova deployments configured with SR-IOV are affected. **CVE ID : CVE-2022-37394**	https://review.opendev.org/c/openstack/nova/+/849985	A-OPE-NOVA-170822/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 24.0.0 Up to (excluding) 24.1.2					
N/A	03-Aug-2022	3.3	An issue was discovered in OpenStack Nova before 23.2.2, 24.x before 24.1.2, and 25.x before 25.0.2. By creating a neutron port with the direct vnic_type, creating an instance bound to that port, and then changing the vnic_type of the bound port to macvtap, an authenticated user may cause the compute service to fail to restart, resulting in a possible denial of service. Only Nova deployments configured with SR-IOV are affected. **CVE ID : CVE-2022-37394**	https://review.opendev.org/c/openstack/nova/+/849985	A-OPE-NOVA-170822/1254
Affected Version(s): From (including) 25.0.0 Up to (excluding) 25.0.2					
N/A	03-Aug-2022	3.3	An issue was discovered in OpenStack Nova before 23.2.2, 24.x before 24.1.2, and 25.x before 25.0.2. By creating a neutron port with the direct vnic_type, creating an instance bound to that port, and then changing the vnic_type of the bound port to	https://review.opendev.org/c/openstack/nova/+/849985	A-OPE-NOVA-170822/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macvtap, an authenticated user may cause the compute service to fail to restart, resulting in a possible denial of service. Only Nova deployments configured with SR-IOV are affected. **CVE ID : CVE-2022-37394**		
Vendor: openzeppelin					
Product: contracts					
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.7.2					
Incorrect Calculation	01-Aug-2022	7.5	OpenZeppelin Contracts is a library for secure smart contract development. This issue concerns instances of Governor that use the module `GovernorVotesQuorumFraction`, a mechanism that determines quorum requirements as a percentage of the voting token's total supply. In affected instances, when a proposal is passed to lower the quorum requirements, past proposals may become executable if they had been defeated only due to lack of quorum, and	https://github.com/OpenZeppelin/openzeppelin-contracts/pull/3561, https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-xrc4-737v-9q75	A-OPE-CONT-170822/1256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the number of votes it received meets the new quorum requirement. Analysis of instances on chain found only one proposal that met this condition, and we are actively monitoring for new occurrences of this particular issue. This issue has been patched in v4.7.2. Users are advised to upgrade. Users unable to upgrade should consider avoiding lowering quorum requirements if a past proposal was defeated for lack of quorum. **CVE ID : CVE-2022-31198**		
Affected Version(s): From (including) 4.6.0 Up to (excluding) 4.7.2					
Incorrect Resource Transfer Between Spheres	01-Aug-2022	5.3	OpenZeppelin Contracts is a library for secure smart contract development. Contracts using the cross chain utilities for Arbitrum L2, `CrossChainEnabled ArbitrumL2` or `LibArbitrumL2`, will classify direct interactions of externally owned accounts (EOAs) as cross chain calls,	https://github.com/OpenZeppelin/openzeppelin-contracts/pull/3578, https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-9j3m-g383-29qr	A-OPE-CONT-170822/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			even though they are not started on L1. This issue has been patched in v4.7.2. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-35916**		
Product: contracts-upgradeable					
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.7.2					
Incorrect Calculation	01-Aug-2022	7.5	OpenZeppelin Contracts is a library for secure smart contract development. This issue concerns instances of Governor that use the module `GovernorVotesQuorumFraction`, a mechanism that determines quorum requirements as a percentage of the voting token's total supply. In affected instances, when a proposal is passed to lower the quorum requirements, past proposals may become executable if they had been defeated only due to lack of quorum, and the number of votes it received meets the new quorum requirement.	https://github.com/OpenZeppelin/openzeppelin-contracts/pull/3561, https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-xrc4-737v-9q75	A-OPE-CONT-170822/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Analysis of instances on chain found only one proposal that met this condition, and we are actively monitoring for new occurrences of this particular issue. This issue has been patched in v4.7.2. Users are advised to upgrade. Users unable to upgrade should consider avoiding lowering quorum requirements if a past proposal was defeated for lack of quorum. **CVE ID : CVE-2022-31198**		
Affected Version(s): From (including) 4.6.0 Up to (excluding) 4.7.2					
Incorrect Resource Transfer Between Spheres	01-Aug-2022	5.3	OpenZeppelin Contracts is a library for secure smart contract development. Contracts using the cross chain utilities for Arbitrum L2, `CrossChainEnabled ArbitrumL2` or `LibArbitrumL2`, will classify direct interactions of externally owned accounts (EOAs) as cross chain calls, even though they are not started on L1. This issue has been patched in v4.7.2.	https://github.com/OpenZeppelin/openzeppelin-contracts/pull/3578, https://github.com/OpenZeppelin/openzeppelin-contracts/security/advisories/GHSA-9j3m-g383-29qr	A-OPE-CONT-170822/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-35916**		
Vendor: Pandorafms					
Product: pandora_fms					
Affected Version(s): * Up to (including) 7.0_ng_759					
Cross-Site Request Forgery (CSRF)	01-Aug-2022	8.8	Pandora FMS v7.0NG.759 allows Cross-Site Request Forgery in Bulk operation (User operation) resulting in elevation of privilege to Administrator group. **CVE ID : CVE-2022-26309**	https://www.incibe.es/en/cve-assignment-publication/coordinated-cves, https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-PAN-PAND-170822/1260
Affected Version(s): * Up to (including) 7.0_ng_760					
N/A	01-Aug-2022	8.8	Pandora FMS v7.0NG.760 and below allows an improper authorization in User Management where any authenticated user with access to the User Management module could create, modify or delete any user with full admin privilege. The impact could lead to a vertical privilege escalation to access the privileges of a higher-level user or	https://www.incibe.es/en/cve-assignment-publication/coordinated-cves, https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-PAN-PAND-170822/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			typically an admin user. **CVE ID : CVE-2022-26310**		
N/A	01-Aug-2022	5.4	Pandora FMS v7.0NG.760 and below allows an improper access control in Configuration (Credential store) where a user with the role of Operator (Write) could create, delete, view existing keys which are outside the intended role. **CVE ID : CVE-2022-26308**	https://www.incibe.es/en/cve-assignment-publication/coordinated-cves, https://pandorafms.com/en/security/common-vulnerabilities-and-exposures/	A-PAN-PAND-170822/1262
Vendor: Percona					
Product: percona_server					
Affected Version(s): 8.0.28-19					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	7.5	An issue in the fetch_step function in Percona Server for MySQL v8.0.28-19 allows attackers to cause a Denial of Service (DoS) via a SQL query. **CVE ID : CVE-2022-34968**	N/A	A-PER-PERC-170822/1263
Vendor: pharmacy_management_system_project					
Product: pharmacy_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL	N/A	A-PHA-PHAR-170822/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			injection vulnerability via the startDate parameter at getproductreport.php. **CVE ID : CVE-2022-34945**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the startDate parameter at getexpproduct.php. **CVE ID : CVE-2022-34946**	N/A	A-PHA-PHAR-170822/1265
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editcategory.php. **CVE ID : CVE-2022-34947**	N/A	A-PHA-PHAR-170822/1266
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editbrand.php. **CVE ID : CVE-2022-34948**	N/A	A-PHA-PHAR-170822/1267
Improper Neutralizat	02-Aug-2022	9.8	Pharmacy Management System	N/A	A-PHA-PHAR-170822/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			v1.0 was discovered to contain multiple SQL injection vulnerabilities via the email or password parameter at login.php. **CVE ID : CVE-2022-34949**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at editproduct.php. **CVE ID : CVE-2022-34950**	N/A	A-PHA-PHAR-170822/1269
Vendor: phptpoint					
Product: pharmacy_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the startDate parameter at getsalereport.php. **CVE ID : CVE-2022-34951**	N/A	A-PHP-PHAR-170822/1270
Improper Neutralization of Special Elements used in an SQL Command	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at edituser.php.	N/A	A-PHP-PHAR-170822/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			**CVE ID : CVE-2022-34952**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the startDate parameter at getOrderReport.php. **CVE ID : CVE-2022-34953**	N/A	A-PHP-PHAR-170822/1272
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pharmacy Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at invoiceprint.php. **CVE ID : CVE-2022-34954**	N/A	A-PHP-PHAR-170822/1273
Vendor: pingcap					
Product: tidb					
Affected Version(s): 6.1.0					
NULL Pointer Dereference	03-Aug-2022	7.5	PingCAP TiDB v6.1.0 was discovered to contain a NULL pointer dereference. **CVE ID : CVE-2022-34969**	https://github.com/pingcap/tidb/issues/35310	A-PIN-TIDB-170822/1274
Vendor: planka					
Product: planka					
Affected Version(s): * Up to (excluding) 1.5.1					
Improper Limitation of a Pathname	04-Aug-2022	6.5	With this vulnerability an attacker can read many sensitive files	https://github.com/plankanban/planka/commit/ac1df5201	A-PLA-PLAN-170822/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			like configuration files, or the /proc/self/environ file, that contains the environment variable used by the web server that includes database credentials. If the web server user is root, an attacker will be able to read any file in the system. **CVE ID : CVE-2022-2653**	dfdaf68d37f7e1b272bc137870d7418, https://huntr.dev/bounties/5dff7cf9-8bb2-4f67-a02d-b94db5009d70	
Vendor: Pligg					
Product: pligg_cms					
Affected Version(s): 2.0.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pligg CMS v2.0.2 was discovered to contain a time-based SQL injection vulnerability via the page_size parameter at load_data_for_topusers.php. **CVE ID : CVE-2022-34955**	N/A	A-PLI-PLIG-170822/1276
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	Pligg CMS v2.0.2 was discovered to contain a time-based SQL injection vulnerability via the page_size parameter at load_data_for_groups.php. **CVE ID : CVE-2022-34956**	N/A	A-PLI-PLIG-170822/1277
Vendor: Postgresql					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: postgresql_jdbc_driver					
Affected Version(s): * Up to (excluding) 42.2.26					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	8	PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard, database independent Java code. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL commands as the application's JDBC user. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that do invoke that method are impacted if the underlying database that they are querying via their JDBC application may be under the control of an	https://github.com/pgjdbc/pgjdbc/commit/739e599d52ad80f8dcd6efedc6157859b1a9d637, https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-r38f-c4h4-hqq2	A-POS-POST-170822/1278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker. The attack requires the attacker to trick the user into executing SQL against a table name who's column names would contain the malicious SQL and subsequently invoke the `refreshRow()` method on the ResultSet. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application that executes as a privileged user querying database schemas owned by potentially malicious less-privileged users would be vulnerable. In that situation it may be possible for the malicious user to craft a schema that causes the application to execute commands as the privileged user. Patched versions will be released as `42.2.26` and `42.4.1`. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31197**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 42.3.0 Up to (excluding) 42.4.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-2022	8	PostgreSQL JDBC Driver (PgJDBC for short) allows Java programs to connect to a PostgreSQL database using standard, database independent Java code. The PGJDBC implementation of the `java.sql.ResultRow.refreshRow()` method is not performing escaping of column names so a malicious column name that contains a statement terminator, e.g. `;`, could lead to SQL injection. This could lead to executing additional SQL commands as the application's JDBC user. User applications that do not invoke the `ResultSet.refreshRow()` method are not impacted. User application that do invoke that method are impacted if the underlying database that they are querying via their JDBC application may be under the control of an attacker. The attack requires the attacker	https://github.com/pgjdbc/pgjdbc/commit/739e599d52ad80f8dcd6efedc6157859b1a9d637, https://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-r38f-c4h4-hqq2	A-POS-POST-170822/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to trick the user into executing SQL against a table name who's column names would contain the malicious SQL and subsequently invoke the `refreshRow()` method on the ResultSet. Note that the application's JDBC user and the schema owner need not be the same. A JDBC application that executes as a privileged user querying database schemas owned by potentially malicious less-privileged users would be vulnerable. In that situation it may be possible for the malicious user to craft a schema that causes the application to execute commands as the privileged user. Patched versions will be released as `42.2.26` and `42.4.1`. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-31197**		
Vendor: Prestashop					
Product: prestashop					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.6.1.10 Up to (excluding) 1.7.8.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Aug-2022	9.8	PrestaShop is an Open Source e-commerce platform. In versions from 1.6.0.10 and before 1.7.8.7 PrestaShop is subject to an SQL injection vulnerability which can be chained to call PHP's Eval function on attacker input. The problem is fixed in version 1.7.8.7. Users are advised to upgrade. Users unable to upgrade may delete the MySQL Smarty cache feature. **CVE ID : CVE-2022-31181**	https://github.com/PrestaShop/PrestaShop/commit/b6d96e7c2a4e35a44e96ffbcdfd34439b56af804, https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-hrgx-p36p-89q4	A-PRE-PRES-170822/1280
Vendor: private_cloud_management_platform_project					
Product: private_cloud_management_platform					
Affected Version(s): -					
Improper Authentication	05-Aug-2022	9.8	A vulnerability classified as critical has been found in Private Cloud Management Platform. Affected is an unknown function of the file /management/api/rcx_management/global_config_query of the component POST Request Handler. The manipulation leads to improper authentication. It is	N/A	A-PRI-PRIV-170822/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to launch the attack remotely. VDB-205614 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2664**		
Vendor: Progress					
Product: ipswitch_ws_ftp_server					
Affected Version(s): * Up to (excluding) 8.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2022	6.1	In Progress WS_FTP Server prior to version 8.7.3, multiple reflected cross-site scripting (XSS) vulnerabilities exist in the administrative web interface. It is possible for a remote attacker to inject arbitrary JavaScript into a WS_FTP administrator's web session. This would allow the attacker to execute code within the context of the victim's browser. **CVE ID : CVE-2022-36967**	https://community.progress.com/s/article/WS-FTP-Server-Critical-Security-Product-Alert-Bulletin-June-2022, https://www.progress.com/ws_ftp	A-PRO-IPSW-170822/1282
Cross-Site Request Forgery (CSRF)	02-Aug-2022	4.3	In Progress WS_FTP Server prior to version 8.7.3, forms within the administrative interface did not include a nonce to mitigate the risk of cross-site request	https://community.progress.com/s/article/WS-FTP-Server-Critical-Security-Product-Alert-Bulletin-June-2022, https://www.p	A-PRO-IPSW-170822/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			forgery (CSRF) attacks. **CVE ID : CVE-2022-36968**	rogress.com/ws_ftp	
Vendor: project-source-code-download_project					
Product: project-source-code-download					
Affected Version(s): 1.0.0					
Files or Directories Accessible to External Parties	01-Aug-2022	7.5	The Project Source Code Download WordPress plugin through 1.0.0 does not protect its backup generation and download functionalities, which may allow any visitors on the site to download the entire site, including sensitive files like wp-config.php. **CVE ID : CVE-2022-1585**	N/A	A-PRO-PROJ-170822/1284
Vendor: pyrocms					
Product: pyrocms					
Affected Version(s): * Up to (including) 3.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	6.1	PyroCMS v3.9 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities. **CVE ID : CVE-2022-35118**	N/A	A-PYR-PYRO-170822/1285
Vendor: Quest					
Product: kace_systems_management_appliance					
Affected Version(s): * Up to (excluding) 12.1.168					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Aug-2022	9.8	A SQL injection vulnerability exists within Quest KACE Systems Management Appliance (SMA) through 12.0 that can allow for remote code execution via download_agent_installer.php. **CVE ID : CVE-2022-29807**	https://support.quest.com/kb/338162, https://support.quest.com/kace-systems-management-appliance/kb/338162/quest-response-to-kace-sma-vulnerabilities-cve-2022-29807	A-QUE-KACE-170822/1286
Insufficiently Protected Credentials	02-Aug-2022	9.8	In Quest KACE Systems Management Appliance (SMA) through 12.0, a hash collision is possible during authentication. This may allow authentication with invalid credentials. **CVE ID : CVE-2022-30285**	https://www.quest.com/kace/, https://support.quest.com/kace-systems-management-appliance/kb/338232/quest-response-to-kace-sma-vulnerabilities-cve-2022-30285	A-QUE-KACE-170822/1287
Use of Insufficiently Random Values	02-Aug-2022	7.5	In Quest KACE Systems Management Appliance (SMA) through 12.0, predictable token generation occurs when appliance linking is enabled. **CVE ID : CVE-2022-29808**	https://support.quest.com/kb/338163, https://support.quest.com/kace-systems-management-appliance/kb/338163/quest-response-to-kace-sma-vulnerabilities-cve-2022-29808	A-QUE-KACE-170822/1288
Vendor: raneto_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: raneto					
Affected Version(s): * Up to (excluding) 0.17.1					
Weak Password Requirements	04-Aug-2022	9.8	Renato v0.17.0 employs weak password complexity requirements, allowing attackers to crack user passwords via brute-force attacks. **CVE ID : CVE-2022-35143**	https://gainsec.com/2022/08/04/cve-2022-35142-cve-2022-35143-cve-2022-35144/	A-RAN-RANE-170822/1289
Improper Authentication	04-Aug-2022	7.5	An issue in Renato v0.17.0 allows attackers to cause a Denial of Service (DoS) via a crafted payload injected into the Search parameter. **CVE ID : CVE-2022-35142**	https://gainsec.com/2022/08/04/cve-2022-35142-cve-2022-35143-cve-2022-35144/	A-RAN-RANE-170822/1290
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-2022	4.8	Renato v0.17.0 was discovered to contain a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2022-35144**	https://gainsec.com/2022/08/04/cve-2022-35142-cve-2022-35143-cve-2022-35144/	A-RAN-RANE-170822/1291
Vendor: rashim					
Product: michlol					
Affected Version(s): * Up to (excluding) 187.4392					
Authorization Bypass Through User-Controlled Key	05-Aug-2022	5.5	Michlol - rashim web interface Insecure direct object references (IDOR). First of all, the attacker needs to login. After he	N/A	A-RAS-MICH-170822/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			performs log into the system there are some functionalities that the specific user is not allowed to perform. However all the attacker needs to do in order to achieve his goals is to change the value of the ptMsl parameter and then the attacker can access sensitive data that he not supposed to access because its belong to another user. **CVE ID : CVE-2022-34769**		
Vendor: Redhat					
Product: integration_camel_k					
Affected Version(s): -					
Uncontrolled Resource Consumption	05-Aug-2022	7.5	When a POST request comes through AJP and the request exceeds the max-post-size limit (maxEntitySize), Undertow's AjpServerRequestConduit implementation closes a connection without sending any response to the client/proxy. This behavior results in that a front-end proxy marking the backend worker (application server)	https://bugzilla.redhat.com/show_bug.cgi?id=2095862&comment#0, https://issues.redhat.com/browse/UNDERTOW-2133	A-RED-INTE-170822/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as an error state and not forward requests to the worker for a while. In mod_cluster, this continues until the next STATUS request (10 seconds intervals) from the application server updates the server state. So, in the worst case, it can result in "All workers are in error state" and mod_cluster responds "503 Service Unavailable" for a while (up to 10 seconds). In mod_proxy_balancer, it does not forward requests to the worker until the "retry" timeout passes. However, luckily, mod_proxy_balancer has "forcerecovery" setting (On by default; this parameter can force the immediate recovery of all workers without considering the retry parameter of the workers if all workers of a balancer are in error state.). So, unlike mod_cluster, mod_proxy_balancer does not result in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			responding "503 Service Unavailable". An attacker could use this behavior to send a malicious request and trigger server errors, resulting in DoS (denial of service). This flaw was fixed in Undertow 2.2.19.Final, Undertow 2.3.0.Alpha2. **CVE ID : CVE-2022-2053**		
Product: jboss_fuse					
Affected Version(s): 7.0.0					
Uncontrolled Resource Consumption	05-Aug-2022	7.5	When a POST request comes through AJP and the request exceeds the max-post-size limit (maxEntitySize), Undertow's AjpServerRequestConduit implementation closes a connection without sending any response to the client/proxy. This behavior results in that a front-end proxy marking the backend worker (application server) as an error state and not forward requests to the worker for a while. In mod_cluster, this continues until the	https://bugzilla.redhat.com/show_bug.cgi?id=2095862&comment#0, https://issues.redhat.com/browse/UNDERTOW-2133	A-RED-JBOS-170822/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			next STATUS request (10 seconds intervals) from the application server updates the server state. So, in the worst case, it can result in "All workers are in error state" and mod_cluster responds "503 Service Unavailable" for a while (up to 10 seconds). In mod_proxy_balancer, it does not forward requests to the worker until the "retry" timeout passes. However, luckily, mod_proxy_balancer has "forcerecovery" setting (On by default; this parameter can force the immediate recovery of all workers without considering the retry parameter of the workers if all workers of a balancer are in error state.). So, unlike mod_cluster, mod_proxy_balancer does not result in responding "503 Service Unavailable". An attacker could use this behavior to send a malicious request and trigger		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server errors, resulting in DoS (denial of service). This flaw was fixed in Undertow 2.2.19.Final, Undertow 2.3.0.Alpha2. **CVE ID : CVE-2022-2053**		
Product: keycloak					
Affected Version(s): 18.0.0					
N/A	05-Aug-2022	7.2	An issue was discovered in Keycloak that allows arbitrary Javascript to be uploaded for the SAML protocol mapper even if the UPLOAD_SCRIPTS feature is disabled **CVE ID : CVE-2022-2668**	https://access.redhat.com/security/cve/CVE-2022-2668	A-RED-KEYC-170822/1295
Product: process_automation_manager					
Affected Version(s): * Up to (excluding) 7.13.1					
XML Injection (aka Blind XPath Injection)	10-Aug-2022	8.2	XML external entity injection(XXE) is a vulnerability that allows an attacker to interfere with an application's processing of XML data. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. The software processes	https://bugzilla.redhat.com/show_bug.cgi?id=2107994#c0	A-RED-PROC-170822/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output. Here, XML external entity injection lead to External Service interaction & Internal file read in Business Central and also Kie-Server APIs. **CVE ID : CVE-2022-2458**		
Product: single_sign-on					
Affected Version(s): 7.0					
N/A	05-Aug-2022	7.2	An issue was discovered in Keycloak that allows arbitrary Javascript to be uploaded for the SAML protocol mapper even if the UPLOAD_SCRIPTS feature is disabled **CVE ID : CVE-2022-2668**	https://access.redhat.com/security/cve/CVE-2022-2668	A-RED-SING-170822/1297
Product: undertow					
Affected Version(s): * Up to (excluding) 2.2.19					
Uncontrolled Resource Consumption	05-Aug-2022	7.5	When a POST request comes through AJP and the request exceeds the max-post-size limit (maxEntitySize),	https://bugzilla.redhat.com/show_bug.cgi?id=2095862&comment#0, https://issues.r	A-RED-UNDE-170822/1298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Undertow's AjpServerRequestConduit implementation closes a connection without sending any response to the client/proxy. This behavior results in that a front-end proxy marking the backend worker (application server) as an error state and not forward requests to the worker for a while. In mod_cluster, this continues until the next STATUS request (10 seconds intervals) from the application server updates the server state. So, in the worst case, it can result in "All workers are in error state" and mod_cluster responds "503 Service Unavailable" for a while (up to 10 seconds). In mod_proxy_balancer, it does not forward requests to the worker until the "retry" timeout passes. However, luckily, mod_proxy_balancer has "forcerecovery" setting (On by default; this	edhat.com/browse/UNDERTOW-2133	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter can force the immediate recovery of all workers without considering the retry parameter of the workers if all workers of a balancer are in error state.). So, unlike mod_cluster, mod_proxy_balancer does not result in responding "503 Service Unavailable". An attacker could use this behavior to send a malicious request and trigger server errors, resulting in DoS (denial of service). This flaw was fixed in Undertow 2.2.19.Final, Undertow 2.3.0.Alpha2. **CVE ID : CVE-2022-2053**		
Affected Version(s): 2.3.0					
Uncontrolled Resource Consumption	05-Aug-2022	7.5	When a POST request comes through AJP and the request exceeds the max-post-size limit (maxEntitySize), Undertow's AjpServerRequestConduit implementation closes a connection without sending any response to the	https://bugzilla.redhat.com/show_bug.cgi?id=2095862&comment#0, https://issues.redhat.com/browse/UNDERTOW-2133	A-RED-UNDE-170822/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			client/proxy. This behavior results in that a front-end proxy marking the backend worker (application server) as an error state and not forward requests to the worker for a while. In mod_cluster, this continues until the next STATUS request (10 seconds intervals) from the application server updates the server state. So, in the worst case, it can result in "All workers are in error state" and mod_cluster responds "503 Service Unavailable" for a while (up to 10 seconds). In mod_proxy_balancer, it does not forward requests to the worker until the "retry" timeout passes. However, luckily, mod_proxy_balancer has "forcerecovery" setting (On by default; this parameter can force the immediate recovery of all workers without considering the retry parameter of the workers if all		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workers of a balancer are in error state.). So, unlike mod_cluster, mod_proxy_balancer does not result in responding "503 Service Unavailable". An attacker could use this behavior to send a malicious request and trigger server errors, resulting in DoS (denial of service). This flaw was fixed in Undertow 2.2.19.Final, Undertow 2.3.0.Alpha2. **CVE ID : CVE-2022-2053**		
Vendor: rich-web					
Product: event_timeline					
Affected Version(s): * Up to (including) 1.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	4.8	The Event Timeline WordPress plugin through 1.1.5 does not sanitize and escape Timeline Text, which could allow high-privileged users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed **CVE ID : CVE-2022-1324**	N/A	A-RIC-EVEN-170822/1300
Vendor: rigatur					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: online_booking_and_hotel_management_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	8.8	A vulnerability was found in Rigatur Online Booking and Hotel Management System aff6409. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file login.php of the component POST Request Handler. The manipulation of the argument email/pass 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-205657 was assigned to this vulnerability. **CVE ID : CVE-2022-2673**	N/A	A-RIG-ONLI-170822/1301
Vendor: rough_chart_project					
Product: rough_chart					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation	08-Aug-2022	4.8	The Rough Chart WordPress plugin through 1.0.0 does not properly escape chart data label, which could allow high privilege users to perform Cross-Site Scripting attacks	N/A	A-ROU-ROUG-170822/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-2409**		
Vendor: rust-websocket_project					
Product: rust-websocket					
Affected Version(s): * Up to (excluding) 0.26.5					
Uncontrolled Resource Consumption	01-Aug-2022	7.5	Rust-WebSocket is a WebSocket (RFC6455) library written in Rust. In versions prior to 0.26.5 untrusted websocket connections can cause an out-of-memory (OOM) process abort in a client or a server. The root cause of the issue is during dataframe parsing. Affected versions would allocate a buffer based on the declared dataframe size, which may come from an untrusted source. When `Vec::with_capacity` fails to allocate, the default Rust allocator will abort the current process, killing all threads. This affects only sync (non-Tokio) implementation. Async version also	https://github.com/websockets-rs/rust-websocket/commit/cbf6e9983e839d2ecad86de8cd1b3f20ed43390b, https://github.com/websockets-rs/rust-websocket/security/advisories/GHSA-qrjv-rf5q-qpxc	A-RUS-RUST-170822/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not limit memory, but does not use `with_capacity`, so DoS can happen only when bytes for oversized dataframe or message actually got delivered by the attacker. The crashes are fixed in version 0.26.5 by imposing default dataframe size limits. Affected users are advised to update to this version. Users unable to upgrade are advised to filter websocket traffic externally or to only accept trusted traffic. **CVE ID : CVE-2022-35922**		
Vendor: Samba					
Product: rsync					
Affected Version(s): * Up to (excluding) 3.2.5					
Missing Authorization	02-Aug-2022	7.4	An issue was discovered in rsync before 3.2.5 that allows malicious remote servers to write arbitrary files inside the directories of connecting peers. The server chooses which files/directories are sent to the client. However, the rsync client performs insufficient	http://www.openwall.com/lists/oss-security/2022/08/02/1	A-SAM-RSYN-170822/1304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of file names. A malicious rsync server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the rsync client target directory and subdirectories (for example, overwrite the .ssh/authorized_keys file). **CVE ID : CVE-2022-29154**		
Vendor: Samsung					
Product: cameralyzer					
Affected Version(s): * Up to (excluding) 3.2.22					
Improper Privilege Management	05-Aug-2022	3.3	Improper access control vulnerability in WebApp in Cameralyzer prior to versions 3.2.22, 3.3.22, 3.4.22 and 3.5.51 allows attackers to access external storage as Cameralyzer privilege. **CVE ID : CVE-2022-36832**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-CAME-170822/1305
Affected Version(s): From (including) 3.3.0 Up to (excluding) 3.3.22					
Improper Privilege Management	05-Aug-2022	3.3	Improper access control vulnerability in WebApp in Cameralyzer prior to versions 3.2.22, 3.3.22, 3.4.22 and 3.5.51 allows attackers to access	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-CAME-170822/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			external storage as Cameralyzer privilege. **CVE ID : CVE-2022-36832**		
Affected Version(s): From (including) 3.4.0 Up to (excluding) 3.4.22					
Improper Privilege Management	05-Aug-2022	3.3	Improper access control vulnerability in WebApp in Cameralyzer prior to versions 3.2.22, 3.3.22, 3.4.22 and 3.5.51 allows attackers to access external storage as Cameralyzer privilege. **CVE ID : CVE-2022-36832**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-CAME-170822/1307
Affected Version(s): From (including) 3.5.0 Up to (excluding) 3.5.51					
Improper Privilege Management	05-Aug-2022	3.3	Improper access control vulnerability in WebApp in Cameralyzer prior to versions 3.2.22, 3.3.22, 3.4.22 and 3.5.51 allows attackers to access external storage as Cameralyzer privilege. **CVE ID : CVE-2022-36832**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-CAME-170822/1308
Product: charm					
Affected Version(s): * Up to (excluding) 1.2.3					
Missing Authorization	05-Aug-2022	5.5	Sensitive information exposure in onCharacteristicChanged in Charm by Samsung prior to	https://security.samsungmobile.com/serviceWeb.smsb?year	A-SAM-CHAR-170822/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 1.2.3 allows attacker to get bluetooth connection information without permission. **CVE ID : CVE-2022-33734**	==2022&month=08	
Missing Authorization	05-Aug-2022	3.3	Sensitive information exposure in onCharacteristicRead in Charm by Samsung prior to version 1.2.3 allows attacker to get bluetooth connection information without permission. **CVE ID : CVE-2022-33733**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-CHAR-170822/1310
Product: checkout					
Affected Version(s): * Up to (excluding) 5.0.53.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	5.5	SQL injection vulnerability via IAPService in Samsung Checkout prior to version 5.0.53.1 allows attackers to access IAP information. **CVE ID : CVE-2022-36839**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-CHEC-170822/1311
Product: galaxy_wearable					
Affected Version(s): * Up to (excluding) 2.2.50					
N/A	05-Aug-2022	4.6	Implicit Intent hijacking vulnerability in Galaxy Wearable prior to version 2.2.50 allows attacker to get	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-GALA-170822/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information. **CVE ID : CVE-2022-36838**		
Product: gameoptimizingservice					
Affected Version(s): * Up to (excluding) 3.3.04.0					
Improper Privilege Management	05-Aug-2022	7.8	Improper Privilege Management vulnerability in Game Optimizing Service prior to versions 3.3.04.0 in Android 10, and 3.5.04.8 in Android 11 and above allows local attacker to execute hidden function for developer by changing package name. **CVE ID : CVE-2022-36833**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-GAME-170822/1313
Affected Version(s): * Up to (excluding) 3.5.04.8					
Improper Privilege Management	05-Aug-2022	7.8	Improper Privilege Management vulnerability in Game Optimizing Service prior to versions 3.3.04.0 in Android 10, and 3.5.04.8 in Android 11 and above allows local attacker to execute hidden function for developer by changing package name. **CVE ID : CVE-2022-36833**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-GAME-170822/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: game_launcher					
Affected Version(s): * Up to (excluding) 6.0.07					
Exposure of Sensitive Information to an Unauthorized Actor	05-Aug-2022	5	Exposure of Sensitive Information vulnerability in Game Launcher prior to version 6.0.07 allows local attacker to access app data with user interaction. **CVE ID : CVE-2022-36834**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-GAME-170822/1315
Product: mtower					
Affected Version(s): * Up to (including) 0.3.0					
Allocation of Resources Without Limits or Throttling	11-Aug-2022	7.5	TEE_Malloc in Samsung mTower through 0.3.0 allows a trusted application to achieve Excessive Memory Allocation via a large len value, as demonstrated by a Numaker-PFM-M2351 TEE kernel crash. **CVE ID : CVE-2022-38155**	N/A	A-SAM-MTOW-170822/1316
Affected Version(s): 0.3.0					
Missing Release of Memory after Effective Lifetime	04-Aug-2022	7.8	The TEE_PopulateTransientObject and __utee_from_attr functions in Samsung mTower 0.3.0 allow a trusted application to trigger a memory overwrite, denial of service, and information	N/A	A-SAM-MTOW-170822/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure by invoking the function TEE_PopulateTransientObject with a large number in the parameter attrCount. **CVE ID : CVE-2022-35858**		
Product: notes					
Affected Version(s): * Up to (excluding) 4.3.14.39					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	5.5	Path traversal vulnerability in UriFileUtils of Samsung Notes prior to version 4.3.14.39 allows attacker to access some file as Samsung Notes permission. **CVE ID : CVE-2022-36831**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-NOTE-170822/1318
Product: samsung_email					
Affected Version(s): * Up to (excluding) 6.1.70.20					
N/A	05-Aug-2022	5.5	Intent redirection vulnerability using implicit intent in Samsung email prior to version 6.1.70.20 allows attacker to get sensitive information. **CVE ID : CVE-2022-36837**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-SAMS-170822/1319
Product: samsung_internet_browser					
Affected Version(s): * Up to (excluding) 17.0.7.34					
N/A	05-Aug-2022	4	Implicit Intent hijacking vulnerability in Samsung Internet Browser prior to	https://security.samsungmobile.com/serviceWeb.smsb?year	A-SAM-SAMS-170822/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 17.0.7.34 allows attackers to access arbitrary files. **CVE ID : CVE-2022-36835**	==2022&month=08	
Product: update					
Affected Version(s): * Up to (excluding) 2.2.9.50					
Uncontrolled Search Path Element	05-Aug-2022	7.3	DLL hijacking vulnerability in Samsung Update Setup prior to version 2.2.9.50 allows attackers to execute arbitrary code. **CVE ID : CVE-2022-36840**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	A-SAM-UPDA-170822/1321
Vendor: sanic_project					
Product: sanic					
Affected Version(s): * Up to (excluding) 20.12.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Aug-2022	7.5	Sanic is an opensource python web server/framework. Affected versions of sanic allow access to lateral directories when using `app.static` if using encoded `%2F` URLs. Parent directory traversal is not impacted. Users are advised to upgrade. There is no known workaround for this issue. **CVE ID : CVE-2022-35920**	https://github.com/sanic-org/sanic/security/advisories/GHSA-8cw9-5hmv-77w6, https://github.com/sanic-org/sanic/pull/2495	A-SAN-SANI-170822/1322
Affected Version(s): From (including) 21.0.0 Up to (excluding) 21.12.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Aug-2022	7.5	Sanic is an opensource python web server/framework. Affected versions of sanic allow access to lateral directories when using `app.static` if using encoded `%2F` URLs. Parent directory traversal is not impacted. Users are advised to upgrade. There is no known workaround for this issue. **CVE ID : CVE-2022-35920**	https://github.com/sanic-org/sanic/security/advisories/GHSA-8cw9-5hmv-77w6, https://github.com/sanic-org/sanic/pull/2495	A-SAN-SANI-170822/1323
Affected Version(s): From (including) 22.0.0 Up to (excluding) 22.6.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Aug-2022	7.5	Sanic is an opensource python web server/framework. Affected versions of sanic allow access to lateral directories when using `app.static` if using encoded `%2F` URLs. Parent directory traversal is not impacted. Users are advised to upgrade. There is no known workaround for this issue. **CVE ID : CVE-2022-35920**	https://github.com/sanic-org/sanic/security/advisories/GHSA-8cw9-5hmv-77w6, https://github.com/sanic-org/sanic/pull/2495	A-SAN-SANI-170822/1324
Vendor: santesoft					
Product: dicom_viewer_pro					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.9.2					
Out-of-bounds Write	03-Aug-2022	7.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.9.2. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16679. **CVE ID : CVE-2022-28668**	N/A	A-SAN-DICO-170822/1325
Product: sante_pacs_server					
Affected Version(s): 3.0.4					
Improper Neutralization of Special Elements used in an SQL	03-Aug-2022	9.8	This vulnerability allows remote attackers to bypass authentication on affected installations of Sante PACS Server 3.0.4. Authentication	N/A	A-SAN-SANT-170822/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			is not required to exploit this vulnerability. The specific flaw exists within the processing of calls to the login endpoint. When parsing the username element, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-17331. **CVE ID : CVE-2022-2272**		
Vendor: SAP					
Product: authenticator					
Affected Version(s): * Up to (excluding) 1.2.17					
N/A	10-Aug-2022	7.5	Under certain conditions SAP Authenticator for Android allows an attacker to access information which would otherwise be restricted. **CVE ID : CVE-2022-35290**	https://launchpad.support.sap.com/#/notes/3216653, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-AUTH-170822/1327
Product: businessobjects_business_intelligence					
Affected Version(s): 420					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	10-Aug-2022	8.2	SAP BusinessObjects Business Intelligence Platform (Open Document) - versions 430, 430, allows an unauthenticated attacker to retrieve sensitive information plain text over the network. On successful exploitation, the attacker can view any data available for a business user and put load on the application by an automated attack. Thus, completely compromising confidentiality but causing a limited impact on the availability of the application. **CVE ID : CVE-2022-32245**	https://launchpad.support.sap.com/#/notes/3210823, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170822/1328
Affected Version(s): 430					
Cleartext Transmission of Sensitive Information	10-Aug-2022	8.2	SAP BusinessObjects Business Intelligence Platform (Open Document) - versions 430, 430, allows an unauthenticated attacker to retrieve sensitive information plain text over the network. On successful exploitation, the attacker can view	https://launchpad.support.sap.com/#/notes/3210823, https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html	A-SAP-BUSI-170822/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			any data available for a business user and put load on the application by an automated attack. Thus, completely compromising confidentiality but causing a limited impact on the availability of the application. **CVE ID : CVE-2022-32245**		
Product: enable_now_manager					
Affected Version(s): 1.0					
Missing Authorization	10-Aug-2022	9.1	Due to insecure session management, SAP Enable Now allows an unauthenticated attacker to gain access to user's account. On successful exploitation, an attacker can view or modify user data causing limited impact on confidentiality and integrity of the application. **CVE ID : CVE-2022-35293**	https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html, https://launchpad.support.sap.com/#/notes/3210566	A-SAP-ENAB-170822/1330
Vendor: securebit					
Product: invitation_based_registrations					
Affected Version(s): * Up to (including) 2.2.84					
Improper Neutralization of	01-Aug-2022	4.8	The Invitation Based Registrations WordPress plugin	N/A	A-SEC-INVI-170822/1331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			through 2.2.84 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 when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2325**		
Vendor: Sem-cms					
Product: Semcms					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2022	9.8	A vulnerability classified as critical has been found in SEMCMS. This affects an unknown part of the file Ant_Check.php. The manipulation of the argument DID 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-205839. **CVE ID : CVE-2022-2726**	N/A	A-SEM-SEMC-170822/1332
Vendor: shescape_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: shescape					
Affected Version(s): * Up to (excluding) 1.5.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Aug-2022	9.8	Shescape is a simple shell escape package for JavaScript. Versions prior to 1.5.8 were found to be subject to code injection on windows. This impacts users that use Shescape (any API function) to escape arguments for cmd.exe on Windows An attacker can omit all arguments following their input by including a line feed character (`'\n'`) in the payload. This bug has been patched in [v1.5.8] which you can upgrade to now. No further changes are required. Alternatively, line feed characters (`'\n'`) can be stripped out manually or the user input can be made the last argument (this only limits the impact). **CVE ID : CVE-2022-31179**	https://github.com/ericcornelissen/shescape/security/advisories/GHSA-jjc5-fp7p-6f8w, https://github.com/ericcornelissen/shescape/pull/332	A-SHE-SHES-170822/1333
Affected Version(s): From (including) 1.4.0 Up to (excluding) 1.5.8					
Improper Neutralization of	01-Aug-2022	9.8	Shescape is a simple shell escape package for JavaScript.	https://github.com/ericcornelissen/shescape	A-SHE-SHES-170822/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			Affected versions were found to have insufficient escaping of white space when interpolating output. This issue only impacts users that use the `escape` or `escapeAll` functions with the `interpolation` option set to `true`. The result is that if an attacker is able to include whitespace in their input they can: 1. Invoke shell-specific behaviour through shell-specific special characters inserted directly after whitespace. 2. Invoke shell-specific behaviour through shell-specific special characters inserted or appearing after line terminating characters. 3. Invoke arbitrary commands by inserting a line feed character. 4. Invoke arbitrary commands by inserting a carriage return character. Behaviour number 1 has been patched in [v1.5.7] which you can upgrade to now. No further changes are required. Behaviour number 2,	/pull/322, https://github.com/ericcornelissen/shescape/pull/324, https://github.com/ericcornelissen/shescape/security/advisories/GHSA-44vr-rwwj-p88h	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3, and 4 have been patched in [v1.5.8] which you can upgrade to now. No further changes are required. The best workaround is to avoid having to use the `interpolation: true` option - in most cases using an alternative is possible, see [the recipes](https://github.com/ericcornelissen/shescape#recipes) for recommendations. Alternatively, users may strip all whitespace from user input. Note that this is error prone, for example: for PowerShell this requires stripping `'\u0085'` which is not included in JavaScript's definition of `\s` for Regular Expressions. **CVE ID : CVE-2022-31180**		
Vendor: Shopware					
Product: shopware					
Affected Version(s): From (including) 5.7.0 Up to (excluding) 5.7.14					
Improper Neutralization of Input During Web Page	01-Aug-2022	5.4	Shopware is an open source e-commerce software. In versions from 5.7.0 a persistent cross site scripting (XSS)	https://github.com/shopware/shopware/security/advisories/GHSA-5834-xv5q-cgfw,	A-SHO-SHOP-170822/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability exists in the customer module. Users are recommend to update to the current version 5.7.14. You can get the update to 5.7.14 regularly via the Auto-Updater or directly via the download overview. There are no known workarounds for this issue. **CVE ID : CVE-2022-31148**	https://github.com/shopware/shopware/commit/7875855005648fba7b39371a70816afae2e07daf, https://docs.shopware.com/en/shopware-5-en/security-updates/security-update-07-2022	
Vendor: Siemens					
Product: teamcenter					
Affected Version(s): From (including) 12.4 Up to (excluding) 12.4.0.15					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter consist of a	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality that is vulnerable to command injection. This could potentially allow an attacker to perform remote code execution. **CVE ID : CVE-2022-34660**		
Loop with Unreachable Exit Condition ('Infinite Loop')	10-Aug-2022	7.5	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter is vulnerable to denial of service by entering infinite loops and using up CPU cycles. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2022-34661**	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0.0.10					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter consist of a functionality that is vulnerable to command injection. This could potentially allow an attacker to perform remote code execution. **CVE ID : CVE-2022-34660**	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1338
Loop with Unreachable Exit Condition ('Infinite Loop')	10-Aug-2022	7.5	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter is vulnerable to denial of service by entering infinite loops and using up CPU cycles. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2022-34661**		
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1.0.10					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V14.0.0.2). File Server Cache service in Teamcenter consist of a functionality that is vulnerable to command injection. This could potentially allow an attacker to perform remote code execution. **CVE ID : CVE-2022-34660**		
Loop with Unreachable Exit Condition ('Infinite Loop')	10-Aug-2022	7.5	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter is vulnerable to denial of service by entering infinite loops and using up CPU cycles. This could allow an	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause denial of service condition. **CVE ID : CVE-2022-34661**		
Affected Version(s): From (including) 13.2 Up to (excluding) 13.2.0.9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter consist of a functionality that is vulnerable to command injection. This could potentially allow an attacker to perform remote code execution. **CVE ID : CVE-2022-34660**	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1342
Loop with Unreachable Exit	10-Aug-2022	7.5	A vulnerability has been identified in Teamcenter V12.4	https://cert-portal.siemens.com/productce	A-SIE-TEAM-170822/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			(All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter is vulnerable to denial of service by entering infinite loops and using up CPU cycles. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2022-34661**	rt/pdf/ssa-759952.pdf	
Affected Version(s): From (including) 13.3 Up to (excluding) 13.3.0.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter consist of a functionality that is vulnerable to command injection. This could potentially allow an attacker to perform remote code execution. **CVE ID : CVE-2022-34660**		
Loop with Unreachable Exit Condition ('Infinite Loop')	10-Aug-2022	7.5	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter is	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to denial of service by entering infinite loops and using up CPU cycles. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2022-34661**		
Affected Version(s): From (including) 14.0 Up to (excluding) 14.0.0.2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter consist of a functionality that is vulnerable to command injection. This could potentially allow an attacker to perform remote code execution.	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34660		
Loop with Unreachable Exit Condition ('Infinite Loop')	10-Aug-2022	7.5	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter is vulnerable to denial of service by entering infinite loops and using up CPU cycles. This could allow an attacker to cause denial of service condition. **CVE ID : CVE-2022-34661**	https://cert-portal.siemens.com/productcert/pdf/ssa-759952.pdf	A-SIE-TEAM-170822/1347
Vendor: sigmaplugin					
Product: advanced_wordpress_reset					
Affected Version(s): * Up to (excluding) 1.6					
Improper Neutralization of Input	01-Aug-2022	6.1	The Advanced WordPress Reset WordPress plugin before 1.6 does not	N/A	A-SIG-ADVA-170822/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			escape some generated URLs before outputting them back in href attributes of admin dashboard pages, leading to Reflected Cross-Site Scripting **CVE ID : CVE-2022-2181**		
Vendor: sigstore					
Product: cosign					
Affected Version(s): * Up to (excluding) 1.10.1					
Improper Verification of Cryptographic Signature	04-Aug-2022	9.8	cosign is a container signing and verification utility. In versions prior to 1.10.1 cosign can report a false positive if any attestation exists. `cosign verify-attestation` used with the `--type` flag will report a false positive verification when there is at least one attestation with a valid signature and there are NO attestations of the type being verified (--type defaults to "custom"). This can happen when signing with a standard keypair and with "keyless" signing with Fulcio. This vulnerability can be reproduced with the `distroless.dev/static	https://github.com/sigstore/cosign/commit/c5fda01a8ff33ca981f45a9f13e7fb6bd2080b94, https://github.com/sigstore/cosign/security/advisories/GHSA-vjxv-45g9-9296	A-SIG-COSI-170822/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e2` image. This image has a `vuln` attestation but not an `spdx` attestation. However, if you run `cosign verify-attestation --type=spdx` on this image, it incorrectly succeeds. This issue has been addressed in version 1.10.1 of cosign. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-35929**		
Product: policy_controller					
Affected Version(s): * Up to (excluding) 0.2.1					
Improper Verification of Cryptographic Signature	04-Aug-2022	8.8	PolicyController is a utility used to enforce supply chain policy in Kubernetes clusters. In versions prior to 0.2.1 PolicyController will report a false positive, resulting in an admission when it should not be admitted when there is at least one attestation with a valid signature and there are NO attestations of the type being verified (-	https://github.com/sigstore/policy-controller/commit/e852af36fb7d42678b21d7e97503c25bd1fd05c8, https://github.com/sigstore/policy-controller/security/advisories/GHSA-739f-hw6h-7wq8	A-SIG-POLI-170822/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			-type defaults to "custom"). An example image that can be used to test this is `ghcr.io/distroless/static@sha256:dd7614b5a12bc4d617b223c588b4e0c833402b8f4991fb5702ea83afad1986e2`. Users should upgrade to version 0.2.1 to resolve this issue. There are no workarounds for users unable to upgrade. **CVE ID : CVE-2022-35930**		
Vendor: simple-membership-plugin					
Product: simple_membership					
Affected Version(s): * Up to (excluding) 4.1.3					
Improper Privilege Management	01-Aug-2022	9.8	The Simple Membership WordPress plugin before 4.1.3 allows user to change their membership at the registration stage due to insufficient checking of a user supplied parameter. **CVE ID : CVE-2022-2317**	N/A	A-SIM-SIMP-170822/1351
Improper Privilege Management	01-Aug-2022	8.8	The Simple Membership WordPress plugin before 4.1.3 does not properly validate the membership_level parameter when	N/A	A-SIM-SIMP-170822/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			editing a profile, allowing members to escalate to a higher membership level by using a crafted POST request. **CVE ID : CVE-2022-2273**		
Vendor: simple_e-learning_system_project					
Product: simple_e-learning_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	9.8	A vulnerability was found in SourceCodester Simple E-Learning System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file search.php. The manipulation of the argument searchPost 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-205819. **CVE ID : CVE-2022-2698**	N/A	A-SIM-SIMP-170822/1353
Improper Neutralization of Special Elements used in an	05-Aug-2022	8.8	A vulnerability classified as critical was found in SourceCodester Simple E-Learning System. Affected by	N/A	A-SIM-SIMP-170822/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			this vulnerability is an unknown functionality of the file classroom.php. The manipulation of the argument post_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-205615. **CVE ID : CVE-2022-2665**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	7.5	A vulnerability was found in SourceCodester Simple E-Learning System. It has been classified as critical. Affected is an unknown function of the file comment_frame.php. The manipulation of the argument post_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-205818 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2697**	N/A	A-SIM-SIMP-170822/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	7.5	A vulnerability was found in SourceCodester Simple E-Learning System. It has been rated as critical. Affected by this issue is some unknown functionality of the file /claire_blake. The manipulation of the argument phoneNumber 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-205820. **CVE ID : CVE-2022-2699**	N/A	A-SIM-SIMP-170822/1356
N/A	08-Aug-2022	7.5	A vulnerability was found in SourceCodester Simple E-Learning System. It has been declared as problematic. This vulnerability affects unknown code of the file downloadFiles.php. The manipulation of the argument download leads to information disclosure. The attack can be initiated remotely. The exploit has been	N/A	A-SIM-SIMP-170822/1357

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-205828. **CVE ID : CVE-2022-2704**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	6.1	A vulnerability classified as problematic was found in SourceCodester Simple E-Learning System. This vulnerability affects unknown code of the file /claire_blake. The manipulation of the argument Bio leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-205822 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2701**	N/A	A-SIM-SIMP-170822/1358
Vendor: simple_food_ordering_system_project					
Product: simple_food_ordering_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	05-Aug-2022	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Food Ordering System 1.0. This affects an	N/A	A-SIM-SIMP-170822/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			unknown part of the file /login.php. The manipulation of the argument email/password with the input "><ScRiPt>alert(1)</sCrIpT> 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-205671. **CVE ID : CVE-2022-2683**		
Vendor: simple_online_book_store_system_project					
Product: simple_online_book_store_system					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	11-Aug-2022	9.8	A vulnerability has been found in SourceCodester Simple Online Book Store System and classified as critical. This vulnerability affects unknown code of the file Admin_ add.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. VDB-206014 is the identifier assigned to this vulnerability.	N/A	A-SIM-SIMP-170822/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2746		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Aug-2022	9.8	A vulnerability was found in SourceCodester Simple Online Book Store and classified as critical. This issue affects some unknown processing of the file book.php. The manipulation of the argument book_isbn leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-206015. **CVE ID : CVE-2022-2747**	N/A	A-SIM-SIMP-170822/1361
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Aug-2022	9.8	A vulnerability, which was classified as critical, was found in SourceCodester Simple Online Book Store System. Affected is an unknown function of the file /obs/book.php. The manipulation of the argument bookisbn leads to sql injection. It is possible to launch the attack remotely. VDB-206166 is the identifier assigned to this vulnerability.	N/A	A-SIM-SIMP-170822/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-2770		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-Aug-2022	9.8	A vulnerability has been found in SourceCodester Simple Online Book Store System and classified as critical. Affected by this vulnerability is an unknown functionality of the file /obs/bookPerPub.php. The manipulation of the argument bookisbn leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-206167. **CVE ID : CVE-2022-2771**	N/A	A-SIM-SIMP-170822/1363
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-2022	6.1	A vulnerability was found in SourceCodester Simple Online Book Store System. It has been classified as problematic. Affected is an unknown function of the file /admin/edit.php. The manipulation of the argument eid leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this	N/A	A-SIM-SIMP-170822/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-206016. **CVE ID : CVE-2022-2748**		
Vendor: simple_student_information_system_project					
Product: simple_student_information_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	9.8	A vulnerability was found in SourceCodester Simple Student Information System. It has been rated as critical. This issue affects some unknown processing of the file admin/departments/manage_department.php. The manipulation of the argument id with the input -5756%27%20UNION%20ALL%20SELECT%20NULL,database(),user(),NULL,NULL,NULL,NULL--%20- 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-205829 was assigned to this vulnerability. **CVE ID : CVE-2022-2705**	N/A	A-SIM-SIMP-170822/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Aug-2022	9.8	A vulnerability was found in SourceCodester Simple Student Information System and classified as critical. This issue affects some unknown processing of the file manage_course.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 associated identifier of this vulnerability is VDB-205835. **CVE ID : CVE-2022-2722**	N/A	A-SIM-SIMP-170822/1366
Vendor: socket					
Product: socket.io-client_java					
Affected Version(s): * Up to (excluding) 2.0.1					
NULL Pointer Dereference	02-Aug-2022	7.5	The package io.socket:socket.io-client before 2.0.1 are vulnerable to NULL Pointer Dereference when parsing a packet with with invalid payload format. **CVE ID : CVE-2022-25867**	https://security.snyk.io/vuln/SNYK-JAVA-IOSOCKET-2949738, https://github.com/socketio/socket.io-client-java/commit/e8ffe9d1383736f6a21090ab959a2f4fa5a41284, https://github.	A-SOC-SOCK-170822/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				com/socketio/socket.io-client-java/commit/8664499b6f31154f49783531f778dac5387b766b	
Vendor: solana					
Product: pay					
Affected Version(s): * Up to (excluding) 0.2.1					
Always-Incorrect Control Flow Implementation	01-Aug-2022	5.3	Solana Pay is a protocol and set of reference implementations that enable developers to incorporate decentralized payments into their apps and services. When a Solana Pay transaction is located using a reference key, it may be checked to represent a transfer of the desired amount to the recipient, using the supplied `validateTransfer` function. An edge case regarding this mechanism could cause the validation logic to validate multiple transfers. This issue has been patched as of version `0.2.1`. Users of the Solana Pay SDK should upgrade to it. There are no known	https://github.com/solana-labs/solana-pay/security/advisories/GHSA-j47c-j42c-mwqq, https://github.com/solana-labs/solana-pay/commit/ac6ce0d0a81137700874a8bf5a7caac3be999fad	A-SOL-PAY-170822/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			workarounds for this issue. **CVE ID : CVE-2022-35917**		
Vendor: sourcegraph					
Product: sourcegraph					
Affected Version(s): * Up to (excluding) 3.41.0					
Incorrect Authorization	01-Aug-2022	4.3	Sourcegraph is an opensource code search and navigation engine. In Sourcegraph versions before 3.41.0, it is possible for an attacker to delete other usersâ€™ saved searches due to a bug in the authorization check. The vulnerability does not allow the reading of other usersâ€™ saved searches, only overwriting them with attacker-controlled searches. The issue is patched in Sourcegraph version 3.41.0. There is no workaround for this issue and updating to a secure version is highly recommended. **CVE ID : CVE-2022-31155**	https://github.com/sourcegraph/sourcegraph/commit/2832d7882396a6295ba5803b5ef48dc7d5a24c59, https://github.com/sourcegraph/sourcegraph/security/advisories/GHSA-37qp-9jq6-f6mx	A-SOU-SOUR-170822/1369
Affected Version(s): * Up to (excluding) 3.42.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	01-Aug-2022	4.3	Sourcegraph is an opensource code search and navigation engine. It is possible for an authenticated Sourcegraph user to edit the Code Monitors owned by any other Sourcegraph user. This includes being able to edit both the trigger and the action of the monitor in question. An attacker is not able to read contents of existing code monitors, only override the data. The issue is fixed in Sourcegraph 3.42. There are no workaround for the issue and patching is highly recommended. **CVE ID : CVE-2022-31154**	https://github.com/sourcegraph/sourcegraph/security/advisories/GHSA-5866-hhq9-9hpc, https://github.com/sourcegraph/sourcegraph/pull/37526	A-SOU-SOUR-170822/1370
Vendor: Sqlite					
Product: sqlite					
Affected Version(s): From (including) 1.0.12 Up to (excluding) 3.39.2					
Improper Validation of Array Index	03-Aug-2022	7.5	SQLite 1.0.12 through 3.39.x before 3.39.2 sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.	https://www.sqlite.org/cves.html	A-SQL-SQLI-170822/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35737		
Vendor: storeapps					
Product: affiliate_for_woocommerce					
Affected Version(s): * Up to (excluding) 4.8.0					
Incorrect Authorization	05-Aug-2022	8.8	Multiple Improper Access Control vulnerabilities in StoreApps Affiliate For WooCommerce premium plugin <= 4.7.0 at WordPress. **CVE ID : CVE-2022-25649**	https://dzv365zjfbd8v.cloudfront.net/changelogs/affiliate-for-woocommerce/changelog.txt	A-STO-AFFI-170822/1372
Affected Version(s): * Up to (including) 4.7.0					
Authorization Bypass Through User-Controlled Key	05-Aug-2022	6.5	Authenticated IDOR vulnerability in StoreApps Affiliate For WooCommerce premium plugin <= 4.7.0 at WordPress allows an attacker to change the PayPal email. WooCommerce PayPal Payments plugin (free) should be at least installed to get the extra input field on the user profile page. **CVE ID : CVE-2022-36284**	https://dzv365zjfbd8v.cloudfront.net/changelogs/affiliate-for-woocommerce/changelog.txt	A-STO-AFFI-170822/1373
Vendor: streamlit					
Product: streamlit					
Affected Version(s): From (including) 0.63.0 Up to (excluding) 1.11.1					
Improper Limitation of a Pathname	01-Aug-2022	6.5	Streamlit is a data oriented application development framework for	https://github.com/streamlit/streamlit/security/advisories/	A-STR-STRE-170822/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			python. Users hosting Streamlit app(s) that use custom components are vulnerable to a directory traversal attack that could leak data from their web server file-system such as: server logs, world readable files, and potentially other sensitive information. An attacker can craft a malicious URL with file paths and the streamlit server would process that URL and return the contents of that file. This issue has been resolved in version 1.11.1. Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-35918**	GHSA-v4hr-4jpx-56gc, https://github.com/streamlit/streamlit/commit/80d9979d5f4a00217743d607078a1d867fad8acf	
Vendor: student_information_system_project					
Product: student_information_system					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command	12-Aug-2022	9.8	A vulnerability classified as critical was found in SourceCodester Student Information System. Affected by this vulnerability is an unknown functionality of the	N/A	A-STU-STUD-170822/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			file /admin/students/view_student.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-206245 was assigned to this vulnerability. **CVE ID : CVE-2022-2797**		
Vendor: supersmart					
Product: supersmart.me_-_walk_through					
Affected Version(s): -					
N/A	05-Aug-2022	7.5	Supersmart.me - Walk Through Performing unauthorized actions on other customers. Supersmart.me has a product designed to conduct smart shopping in stores. The customer receives a coder (or using an Android application) to scan at the beginning of the purchase the QR CODE on the cart, and then all the products he wants to purchase. At the end of the purchase the customer can pay independently. During the research it was discovered that it is possible to	N/A	A-SUP-SUPE-170822/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset another customer's cart without verification. Because the number of purchases is serial. **CVE ID : CVE-2022-34768**		
Vendor: Synology					
Product: calendar					
Affected Version(s): * Up to (excluding) 2.3.4-0631					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	4.3	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Calendar before 2.3.4-0631 allows remote authenticated users to download arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27617**	https://www.synology.com/security/advisory/Synology_SA_20_07	A-SYN-CALE-170822/1377
Product: diskstation_manager					
Affected Version(s): 7.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	6.5	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Storage Analyzer before 2.1.0-0390 allows remote authenticated users to delete arbitrary files via unspecified vectors.	https://www.synology.com/security/advisory/Synology_SA_22_11	A-SYN-DISK-170822/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27618		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	4.9	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology SSO Server before 2.2.3-0331 allows remote authenticated users to read arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27620**	https://www.synology.com/security/advisory/Synology_SA_22_13	A-SYN-DISK-170822/1379
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	3.8	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology USB Copy before 2.2.0-1086 allows remote authenticated users to read or write arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27621**	https://www.synology.com/security/advisory/Synology_SA_22_14	A-SYN-DISK-170822/1380
Affected Version(s): 6.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	6.5	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Storage Analyzer before 2.1.0-0390 allows	https://www.synology.com/security/advisory/Synology_SA_22_11	A-SYN-DISK-170822/1381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote authenticated users to delete arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27618**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	4.9	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology SSO Server before 2.2.3-0331 allows remote authenticated users to read arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27620**	https://www.synology.com/security/advisory/Synology_SA_22_13	A-SYN-DISK-170822/1382
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	4.3	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Calendar before 2.3.4-0631 allows remote authenticated users to download arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27617**	https://www.synology.com/security/advisory/Synology_SA_20_07	A-SYN-DISK-170822/1383
Improper Limitation of a Pathname to a	03-Aug-2022	3.8	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in	https://www.synology.com/security/advisory/Synology_SA_22_14	A-SYN-DISK-170822/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			webapi component in Synology USB Copy before 2.2.0-1086 allows remote authenticated users to read or write arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27621**		
Affected Version(s): 7.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	6.5	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Storage Analyzer before 2.1.0-0390 allows remote authenticated users to delete arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27618**	https://www.synology.com/security/advisory/Synology_SA_22_11	A-SYN-DISK-170822/1385
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	4.9	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology SSO Server before 2.2.3-0331 allows remote authenticated users to read arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27620**	https://www.synology.com/security/advisory/Synology_SA_22_13	A-SYN-DISK-170822/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	3.8	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology USB Copy before 2.2.0-1086 allows remote authenticated users to read or write arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27621**	https://www.synology.com/security/advisory/Synology_SA_22_14	A-SYN-DISK-170822/1387
Affected Version(s): From (including) 6.2 Up to (excluding) 6.2.4-25556-5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	03-Aug-2022	7.2	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in webapi component in Synology DiskStation Manager (DSM) before 7.0.1-42218-3 allows remote authenticated users to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-27616**	https://www.synology.com/security/advisory/Synology_SA_22_03	A-SYN-DISK-170822/1388
Affected Version(s): From (including) 7.0 Up to (excluding) 7.0.1-42218-3					
Improper Neutralization of Special Elements used in an	03-Aug-2022	7.2	Improper neutralization of special elements used in an OS command ('OS Command Injection')	https://www.synology.com/security/advisory/Synology_SA_22_03	A-SYN-DISK-170822/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			vulnerability in webapi component in Synology DiskStation Manager (DSM) before 7.0.1-42218-3 allows remote authenticated users to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-27616**		
Product: note_station					
Affected Version(s): * Up to (excluding) 2.2.2-609					
Cleartext Transmission of Sensitive Information	03-Aug-2022	5.9	Cleartext transmission of sensitive information vulnerability in authentication management in Synology Note Station Client before 2.2.2-609 allows man-in-the-middle attackers to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2022-27619**	https://www.synology.com/security/advisory/Synology_SA_22_12	A-SYN-NOTE-170822/1390
Product: sso_server					
Affected Version(s): * Up to (excluding) 2.2.3-0331					
Improper Limitation of a Pathname to a Restricted Directory	03-Aug-2022	4.9	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology SSO Server before 2.2.3-	https://www.synology.com/security/advisory/Synology_SA_22_13	A-SYN-SSO_-170822/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			0331 allows remote authenticated users to read arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27620**		
Product: storage_analyzer					
Affected Version(s): * Up to (excluding) 2.0.1-0214					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	6.5	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Storage Analyzer before 2.1.0-0390 allows remote authenticated users to delete arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27618**	https://www.synology.com/security/advisory/Synology_SA_22_11	A-SYN-STOR-170822/1392
Affected Version(s): * Up to (excluding) 2.1.0-0390					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	6.5	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology Storage Analyzer before 2.1.0-0390 allows remote authenticated users to delete arbitrary files via unspecified vectors.	https://www.synology.com/security/advisory/Synology_SA_22_11	A-SYN-STOR-170822/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27618		
Product: usb_copy					
Affected Version(s): * Up to (excluding) 2.2.0-1086					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-2022	3.8	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology USB Copy before 2.2.0-1086 allows remote authenticated users to read or write arbitrary files via unspecified vectors. **CVE ID : CVE-2022-27621**	https://www.synology.com/security/advisory/Synology_SA_22_14	A-SYN-USB_-170822/1394
Vendor: teamplus					
Product: team\+_pro					
Affected Version(s): * Up to (including) 3.011.6.0.1					
Allocation of Resources Without Limits or Throttling	02-Aug-2022	6.5	Teamplus Pro community discussion function has an 'allocation of resource without limits or throttling' vulnerability. A remote attacker with general user privilege posting a thread with large content can cause the receiving client device to allocate too much memory, leading to abnormal termination of this client's Teamplus Pro application.	N/A	A-TEA-TEAM-170822/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35220		
Allocation of Resources Without Limits or Throttling	02-Aug-2022	5.4	Teamplus Pro community discussion has an 'allocation of resource without limits or throttling' vulnerability on thread subject field. A remote attacker with general user privilege posting a thread subject with large content can cause the server to allocate too much memory, leading to missing partial post content and disrupt partial service. **CVE ID : CVE-2022-35221**	N/A	A-TEA-TEAM-170822/1396
Vendor: Tencent					
Product: tscancode					
Affected Version(s): 2.15.01					
N/A	03-Aug-2022	7.5	A vulnerability in the lua parser of TscanCode tsclua v2.15.01 allows attackers to cause a Denial of Service (DoS) via a crafted lua script. **CVE ID : CVE-2022-35158**	N/A	A-TEN-TSCA-170822/1397
Vendor: thalesgroup					
Product: citadel					
Affected Version(s): * Up to (excluding) 7.1.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Aug-2022	6.1	The embedded neutralization of Script-Related HTML Tag, was by-passed in the case of some extra conditions. **CVE ID : CVE-2022-1293**	https://www.ercom.com/security-updates	A-THA-CITA-170822/1398
Vendor: thinkific					
Product: thinkific_uploader					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The Thinkific Uploader WordPress plugin through 1.0.0 does not sanitise and escape its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks against other administrators. **CVE ID : CVE-2022-2426**	N/A	A-THI-THIN-170822/1399
Vendor: Tibco					
Product: eftl					
Affected Version(s): 6.8.0					
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL -	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-	A-TIB-EFTL-170822/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0.	tibco-ftl-cve-2022-30574	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30574		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.7.3					
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30574	A-TIB-EFTL-170822/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30574**		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.8.0					
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30574	A-TIB-EFTL-170822/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30574**		
Affected Version(s): From (including) 6.0.1 Up to (including) 6.8.0					
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL -	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-	A-TIB-EFTL-170822/1403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0	security-advisory-august-9-2022-tibco-ftl-cve-2022-30574	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30574**		
Product: ftl					
Affected Version(s): 6.8.0					
N/A	09-Aug-2022	8.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, and TIBCO FTL - Enterprise Edition contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a privilege escalation on the affected ftlserver. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO FTL -	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30573	A-TIB-FTL-170822/1404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30573**		
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30574	A-TIB-FTL-170822/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30574**		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.7.3					
N/A	09-Aug-2022	8.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, and TIBCO FTL - Enterprise Edition contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a privilege escalation on the affected ftlserver. Affected releases are TIBCO Software Inc.'s TIBCO FTL -	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30573	A-TIB-FTL-170822/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO FTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30573**		
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30574	A-TIB-FTL-170822/1407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30574**		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.8.0					
N/A	09-Aug-2022	8.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, and TIBCO FTL - Enterprise Edition contains an easily	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-	A-TIB-FTL-170822/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability that allows a low privileged attacker with network access to execute a privilege escalation on the affected ftlserver. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO FTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30573**	tibco-ftl-cve-2022-30573	
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition,	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30574	A-TIB-FTL-170822/1409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30574**		
Affected Version(s): From (including) 6.0.1 Up to (including) 6.8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	8.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition, TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, and TIBCO FTL - Enterprise Edition contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a privilege escalation on the affected ftlserver. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO FTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30573**	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30573	A-TIB-FTL-170822/1410
N/A	09-Aug-2022	7.8	The ftlserver component of TIBCO Software Inc.'s TIBCO FTL - Community Edition,	https://www.tibco.com/services/support/advisories, https://www.ti	A-TIB-FTL-170822/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TIBCO FTL - Developer Edition, TIBCO FTL - Enterprise Edition, TIBCO FTL - Enterprise Edition, TIBCO eFTL - Community Edition, TIBCO eFTL - Developer Edition, TIBCO eFTL - Enterprise Edition, and TIBCO eFTL - Enterprise Edition contains a difficult to exploit vulnerability that allows a low privileged attacker with local access to obtain user credentials to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO FTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO FTL - Developer Edition: versions 6.0.1 through 6.8.0, TIBCO FTL - Enterprise Edition: versions 6.0.0 through 6.7.3, TIBCO FTL - Enterprise Edition: version 6.8.0, TIBCO eFTL - Community Edition: versions 6.0.0 through 6.8.0, TIBCO eFTL - Developer Edition: versions 6.0.1 through 6.8.0,	bco.com/support/advisories/2022/08/tibco-security-advisory-august-9-2022-tibco-ftl-cve-2022-30574	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			TIBCO eFTL - Enterprise Edition: versions 6.0.0 through 6.7.3, and TIBCO eFTL - Enterprise Edition: version 6.8.0. **CVE ID : CVE-2022-30574**		
Product: iway_service_manager					
Affected Version(s): * Up to (excluding) 8.0.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Aug-2022	6.5	The iWay Service Manager Console component of TIBCO Software Inc.'s TIBCO iWay Service Manager contains an easily exploitable Directory Traversal vulnerability that allows a low privileged attacker with network access to read arbitrary resources on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO iWay Service Manager: versions 8.0.6 and below. **CVE ID : CVE-2022-30572**	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/07/tibco-security-advisory-august-2-2022-tibco-iway-sm-cve-2022-30572	A-TIB-IWAY-170822/1412
Improper Neutralization of Input During Web Page Generation	02-Aug-2022	5.4	The iWay Service Manager Console component of TIBCO Software Inc.'s TIBCO iWay Service Manager contains easily exploitable Reflected Cross Site	https://www.tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2022/07/tibco-	A-TIB-IWAY-170822/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO iWay Service Manager: versions 8.0.6 and below. **CVE ID : CVE-2022-30571**	security-advisory-august-2-2022-tibco-iway-sm-cve-2022-30571	
Vendor: timersys					
Product: popups					
Affected Version(s): * Up to (including) 1.9.3.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Aug-2022	4.8	The WordPress Popup WordPress plugin through 1.9.3.8 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 when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2305**	N/A	A-TIM-POPU-170822/1414
Vendor: tooljet					
Product: tooljet					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.19.0					
Improper Access Control	02-Aug-2022	8.8	Improper Access Control in GitHub repository tooljet/tooljet prior to v1.19.0. **CVE ID : CVE-2022-2631**	https://github.com/tooljet/tooljet/commit/b9fa229bcae356cbb33300b31483e97e6ea140a7, https://huntr.dev/bounties/86881f9e-ca48-49b5-9782-3c406316930c	A-TOO-TOOL-170822/1415
Vendor: triplecross_project					
Product: triplecross					
Affected Version(s): 0.1.0					
Allocation of Resources Without Limits or Throttling	03-Aug-2022	7.5	A segmentation fault in TripleCross v0.1.0 occurs when sending a control command from the client to the server. This occurs because there is no limit to the length of the output of the executed command. **CVE ID : CVE-2022-35505**	N/A	A-TRI-TRIP-170822/1416
Allocation of Resources Without Limits or Throttling	03-Aug-2022	7.5	TripleCross v0.1.0 was discovered to contain a stack overflow which occurs because there is no limit to the length of program parameters. **CVE ID : CVE-2022-35506**	N/A	A-TRI-TRIP-170822/1417
Vendor: typelevel					
Product: fs2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 3.1.0 Up to (excluding) 3.2.11					
Improper Certificate Validation	01-Aug-2022	9.8	fs2 is a compositional, streaming I/O library for Scala. When establishing a server-mode `TLSSocket` using `fs2-io` on Node.js, the parameter `requestCert = true` is ignored, peer certificate verification is skipped, and the connection proceeds. The vulnerability is limited to: 1. `fs2-io` running on Node.js. The JVM TLS implementation is completely independent. 2. `TLSSocket`s in server-mode. Client-mode `TLSSocket`s are implemented via a different API. 3. mTLS as enabled via `requestCert = true` in `TLSParameters`. The default setting is `false` for server-mode `TLSSocket`s. It was introduced with the initial Node.js implementation of fs2-io in 3.1.0. A patch is released in v3.2.11. The requestCert = true parameter is respected and the	https://github.com/typelevel/fs2/security/advisories/GHSA-2cpx-6pqp-wf35, https://github.com/typelevel/fs2/commit/659824395826a314e0a4331535dbf1ef8bef8207	A-TYP-FS2-170822/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			peer certificate is verified. If verification fails, a SSLException is raised. If using an unpatched version on Node.js, do not use a server-mode TLSSocket with requestCert = true to establish a mTLS connection. **CVE ID : CVE-2022-31183**		
Vendor: typescript_deep_merge_project					
Product: typescript_deep_merge					
Affected Version(s): * Up to (excluding) 2.0.2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	09-Aug-2022	9.8	The package ts-deepmerge before 2.0.2 are vulnerable to Prototype Pollution due to missing sanitization of the merge function. **CVE ID : CVE-2022-25907**	https://github.com/voodoocreation/ts-deepmerge/commit/9be5148773343c57be9de39728d6ead18eddf10b, https://github.com/voodoocreation/ts-deepmerge/releases/tag/2.0.2, https://security.snyk.io/vuln/SNYK-JS-TSDEEPMERGE-2959975	A-TYP-TYPE-170822/1419
Vendor: ucms_project					
Product: ucms					
Affected Version(s): 1.6					
Unrestricted Upload of	10-Aug-2022	9.8	UCMS 1.6 is vulnerable to	N/A	A-UCM-UCMS-170822/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			arbitrary file upload via ucms/sadmin/file PHP file. **CVE ID : CVE-2022-35426**		
Vendor: uniwill					
Product: sparkio.sys					
Affected Version(s): 1.0					
Allocation of Resources Without Limits or Throttling	05-Aug-2022	7.8	The Uniwill SparkIO.sys driver 1.0 is vulnerable to a stack-based buffer overflow via IOCTL 0x40002008. **CVE ID : CVE-2022-37415**	N/A	A-UNI-SPAR-170822/1421
Vendor: uthscsa					
Product: multi-image_analysis_gui					
Affected Version(s): 4.1					
N/A	01-Aug-2022	8.8	An issue in \Roaming\Mango\Plugins of University of Texas Multi-image Analysis GUI (Mango) 4.1 allows attackers to escalate privileges via crafted plugins. **CVE ID : CVE-2022-34567**	https://ric.uthscsa.edu/mango/develop.html, https://ric.uthscsa.edu/mango/mango.html, https://ric.uthscsa.edu/mango/index.html	A-UTH-MULT-170822/1422
Vendor: v8n_project					
Product: v8n					
Affected Version(s): * Up to (excluding) 1.5.1					
N/A	02-Aug-2022	7.5	v8n is a javascript validation library. Versions of v8n prior to 1.5.1 were found to have an inefficient	https://github.com/imbrn/v8n/security/advisories/GHSA-xrx9-gj26-	A-V8N-V8N-170822/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			regular expression complexity in the `lowercase()` and `uppercase()` regex which could lead to a denial of service attack. In testing of the `lowercase()` function a payload of 'a' + 'a'.repeat(i) + 'A' with 32 leading characters took 29443 ms to execute. The same issue happens with uppercase(). Users are advised to upgrade. There are no known workarounds for this issue. **CVE ID : CVE-2022-35923**	5wx9, https://github.com/imbrn/v8n/commit/92393862156fad190c05ec3f6e2bc73308dcd2f9	
Vendor: varnish_cache_project					
Product: varnish_cache					
Affected Version(s): 7.0.0					
N/A	11-Aug-2022	7.5	In Varnish Cache 7.0.0, 7.0.1, 7.0.2, and 7.1.0, it is possible to cause the Varnish Server to assert and automatically restart through forged HTTP/1 backend responses. An attack uses a crafted reason phrase of the backend response status line. This is fixed in 7.0.3 and 7.1.1.	https://varnish-cache.org/security/VSV00009.html	A-VAR-VARN-170822/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-38150		
Affected Version(s): 7.1.0					
N/A	11-Aug-2022	7.5	In Varnish Cache 7.0.0, 7.0.1, 7.0.2, and 7.1.0, it is possible to cause the Varnish Server to assert and automatically restart through forged HTTP/1 backend responses. An attack uses a crafted reason phrase of the backend response status line. This is fixed in 7.0.3 and 7.1.1. **CVE ID : CVE-2022-38150**	https://varnish-cache.org/security/VSV00009.html	A-VAR-VARN-170822/1425
Affected Version(s): 7.0.1					
N/A	11-Aug-2022	7.5	In Varnish Cache 7.0.0, 7.0.1, 7.0.2, and 7.1.0, it is possible to cause the Varnish Server to assert and automatically restart through forged HTTP/1 backend responses. An attack uses a crafted reason phrase of the backend response status line. This is fixed in 7.0.3 and 7.1.1. **CVE ID : CVE-2022-38150**	https://varnish-cache.org/security/VSV00009.html	A-VAR-VARN-170822/1426
Affected Version(s): 7.0.2					
N/A	11-Aug-2022	7.5	In Varnish Cache 7.0.0, 7.0.1, 7.0.2, and	https://varnish-	A-VAR-VARN-170822/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.1.0, it is possible to cause the Varnish Server to assert and automatically restart through forged HTTP/1 backend responses. An attack uses a crafted reason phrase of the backend response status line. This is fixed in 7.0.3 and 7.1.1. **CVE ID : CVE-2022-38150**	cache.org/security/VSV00009.html	
Vendor: VIM					
Product: vim					
Affected Version(s): * Up to (excluding) 9.0.0100					
Undefined Behavior for Input to API	01-Aug-2022	5.5	Undefined Behavior for Input to API in GitHub repository vim/vim prior to 9.0.0100. **CVE ID : CVE-2022-2598**	https://github.com/vim/vim/commit/4e677b9c40ccbc5f090971b31dc2fe07bf05541d, https://huntr.dev/bounties/2f08363a-47a2-422d-a7de-ce96a89ad08e	A-VIM-VIM-170822/1428
Affected Version(s): * Up to (excluding) 9.0.0101					
Heap-based Buffer Overflow	01-Aug-2022	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0101. **CVE ID : CVE-2022-2571**	https://github.com/vim/vim/commit/a6f9e300161f4cb54713da22f65b261595e8e614, https://huntr.dev/bounties/2e5a1dc4-2dfb-4e5f-8c70-e1ede21f3571	A-VIM-VIM-170822/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 9.0.0102					
Heap-based Buffer Overflow	01-Aug-2022	7.8	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0102. **CVE ID : CVE-2022-2580**	https://huntr.dev/bounties/c5f2f1d4-0441-4881-b19c-055acaa16249, https://github.com/vim/vim/commit/1e56bda9048a9625bce6e660938c834c5c15b07d	A-VIM-VIM-170822/1430
Affected Version(s): * Up to (excluding) 9.0.0104					
Out-of-bounds Read	01-Aug-2022	7.8	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.0104. **CVE ID : CVE-2022-2581**	https://huntr.dev/bounties/0bedbae2-82ae-46ae-aa68-1c28b309b60b, https://github.com/vim/vim/commit/f50940531dd57135fe60aa393ac9d3281f352d88	A-VIM-VIM-170822/1431
Vendor: vinchin					
Product: vinchin_backup_and_recovery					
Affected Version(s): 6.5.0.17561					
Use of Hard-coded Credentials	03-Aug-2022	9.8	This vulnerability allows remote attackers to bypass authentication on affected installations of Vinchin Backup and Recovery 6.5.0.17561. Authentication is not required to exploit this vulnerability. The specific flaw exists within the configuration of the MySQL server. The	N/A	A-VIN-VINC-170822/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server uses a hard-coded password for the administrator user. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-17139. **CVE ID : CVE-2022-35866**		
Vendor: Vmware					
Product: access_connector					
Affected Version(s): 21.08.0.0					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1433
Improper Neutralization of Special Elements in Output Used by a Downstream	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**		
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1435
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1436
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31664		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1438
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1439
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**		
Affected Version(s): 21.08.0.1					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1441
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1442
Improper Privilege	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation	https://www.vmware.com/security/advisories/VMSA-	A-VMW-ACCE-170822/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	2022-0021.html	
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1444
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1445
Improper Limitation of a Pathname to a Restricted Directory	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1447
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1448
Affected Version(s): 22.05					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1449
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1450
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31660		
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1452
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1453
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1455
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1456
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			target user's window. **CVE ID : CVE-2022-31663**		
Affected Version(s): 22.08.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1458
Affected Version(s): 22.08.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ACCE-170822/1459
Product: identity_manager					
Affected Version(s): 3.3.4					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1461
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1462
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege	https://www.vmware.com/security/advisories/VMSA-	A-VMW-IDEN-170822/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	2022-0021.html	
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1464
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1465
Improper Neutralization of Special Elements in Output Used by a Downstrea	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1467
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1468
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**		
Affected Version(s): 3.3.5					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1470
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1472
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1473
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1474
Improper Limitation of a	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors	https://www.vmware.com/security/advisori	A-VMW-IDEN-170822/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	es/VMSA-2022-0021.html	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1476
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1477
Improper Neutralization of Special Elements	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote	https://www.vmware.com/security/advisories/VMSA-	A-VMW-IDEN-170822/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in Output Used by a Downstream Component ('Injection')			code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	2022-0021.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1479
Affected Version(s): 3.3.6					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1481
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1482
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31661		
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1484
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1485
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1487
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1488
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			target user's window. **CVE ID : CVE-2022-31663**		
Product: identity_manager_connector					
Affected Version(s): 3.3.4					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1490
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1491
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation	https://www.vmware.com/security/advisories/VMSA-	A-VMW-IDEN-170822/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	2022-0021.html	
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1493
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1494
Improper Limitation of a Pathname to a Restricted Directory	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1496
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1497
Improper Neutralization of Special Elements in Output Used by a Downstream	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1499
Affected Version(s): 3.3.5					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31656		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1501
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1502
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1504
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1505
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1506
Improper Neutralizat	05-Aug-2022	7.2	VMware Workspace ONE Access and	https://www.vmware.com/se	A-VMW-IDEN-170822/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	curity/advisories/VMSA-2022-0021.html	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1508
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31663		
Affected Version(s): 3.3.6					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1510
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1511
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**		
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1513
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1514
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31662		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1516
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1517
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31665		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1519
Affected Version(s): 19.03.0.1					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1520
Improper Neutralizat	05-Aug-2022	9.8	VMware Workspace ONE Access and	https://www.vmware.com/se	A-VMW-IDEN-170822/1521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements in Output Used by a Downstream Component ('Injection')			Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	curity/advisories/VMSA-2022-0021.html	
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1522
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1523
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege	https://www.vmware.com/security/advisories/VMSA-	A-VMW-IDEN-170822/1524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	2022-0021.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1525
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1526
Improper Neutralization of Special Elements used in an SQL	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1528
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-IDEN-170822/1529
Product: one_access					
Affected Version(s): 21.08.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1530
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1531
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'.	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31660		
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1533
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1534
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1536
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1537
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1539
Affected Version(s): 21.08.0.1					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1540
Improper Neutralization of Special	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL	https://www.vmware.com/security/advisories/VMSA-	A-VMW-ONE_-170822/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	2022-0021.html	
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1542
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1543
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1545
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1546
Improper Neutralization of Special Elements used in an SQL Command	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			trigger a remote code execution. **CVE ID : CVE-2022-31659**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1548
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	A-VMW-ONE_-170822/1549
Product: vrealize_operations					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.6.4					
Exposure of	10-Aug-2022	8.8	VMware vRealize Operations contains	https://www.vmware.com/se	A-VMW-VREA-170822/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			an information disclosure vulnerability. A low-privileged malicious actor with network access can create and leak hex dumps, leading to information disclosure. Successful exploitation can lead to a remote code execution. **CVE ID : CVE-2022-31673**	curity/advisories/VMSA-2022-0022.html	
Incorrect Authorization	10-Aug-2022	7.5	VMware vRealize Operations contains an authentication bypass vulnerability. An unauthenticated malicious actor with network access may be able to create a user with administrative privileges. **CVE ID : CVE-2022-31675**	https://www.vmware.com/security/advisories/VMSA-2022-0022.html	A-VMW-VREA-170822/1551
Improper Privilege Management	10-Aug-2022	7.2	VMware vRealize Operations contains a privilege escalation vulnerability. A malicious actor with administrative network access can escalate privileges to root. **CVE ID : CVE-2022-31672**	https://www.vmware.com/security/advisories/VMSA-2022-0022.html	A-VMW-VREA-170822/1552
Insertion of Sensitive	10-Aug-2022	4.3	VMware vRealize Operations contains	https://www.vmware.com/se	A-VMW-VREA-170822/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			an information disclosure vulnerability. A low-privileged malicious actor with network access can access log files that lead to information disclosure. **CVE ID : CVE-2022-31674**	curity/advisories/VMSA-2022-0022.html	
Product: workstation					
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.2.4					
Insufficiently Protected Credentials	10-Aug-2022	5.9	VMware Workstation (16.x prior to 16.2.4) contains an unprotected storage of credentials vulnerability. A malicious actor with local user privileges to the victim machine may exploit this vulnerability leading to the disclosure of user passwords of the remote server connected through VMware Workstation. **CVE ID : CVE-2022-22983**	https://www.vmware.com/security/advisories/VMSA-2022-0023.html	A-VMW-WORK-170822/1554
Vendor: web_based_quiz_system_project					
Product: web_based_quiz_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	02-Aug-2022	9.8	Web Based Quiz System v1.0 was discovered to contain a SQL	N/A	A-WEB-WEB_-170822/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			injection vulnerability via the qid parameter at update.php. **CVE ID : CVE-2022-35422**		
Vendor: wedding_hall_booking_system_project					
Product: wedding_hall_booking_system					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2022	5.4	A vulnerability classified as problematic has been found in SourceCodester Wedding Hall Booking System. Affected is an unknown function of the file /whbs/?page=contact_us of the component Contact Page. The manipulation of the argument Message 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-205812. **CVE ID : CVE-2022-2689**	N/A	A-WED-WEDD-170822/1556
Improper Neutralization of Input During	06-Aug-2022	5.4	A vulnerability classified as problematic was found in SourceCodester	N/A	A-WED-WEDD-170822/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Wedding Hall Booking System. Affected by this vulnerability is an unknown functionality of the file /whbs/?page=my_bookings of the component Booking Form. The manipulation of the argument Remarks leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-205813 was assigned to this vulnerability. **CVE ID : CVE-2022-2690**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2022	5.4	A vulnerability, which was classified as problematic, has been found in SourceCodester Wedding Hall Booking System. Affected by this issue is some unknown functionality of the file /whbs/?page=manage_account of the component Profile Page. The manipulation leads to cross site	N/A	A-WED-WEDD-170822/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-205814 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-2691**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Aug-2022	5.4	A vulnerability, which was classified as problematic, was found in SourceCodester Wedding Hall Booking System. This affects an unknown part of the file /whbs/admin/?page=user of the component Staff User Profile. The manipulation of the argument First Name/Last Name 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-205815. **CVE ID : CVE-2022-2692**	N/A	A-WED-WEDD-170822/1559
Vendor: weformspro					
Product: weforms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.6.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The weForms WordPress plugin before 1.6.14 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2022-2395**	N/A	A-WEF-WEFO-170822/1560
Vendor: Wolfssl					
Product: wolfssl					
Affected Version(s): * Up to (excluding) 5.4.0					
N/A	08-Aug-2022	7.5	wolfSSL before 5.4.0 allows remote attackers to cause a denial of service via DTLS because a check for return-routability can be skipped. **CVE ID : CVE-2022-34293**	https://github.com/wolfSSL/wolfssl/releases/tag/v5.4.0-stable	A-WOL-WOLF-170822/1561
Vendor: wow-company					
Product: counter_box					
Affected Version(s): * Up to (excluding) 1.2.1					
Cross-Site Request Forgery (CSRF)	01-Aug-2022	8.8	The Counter Box WordPress plugin before 1.2.1 is lacking CSRF check when activating and deactivating counters, which could allow attackers	N/A	A-WOW-COUN-170822/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to make a logged in admin perform such actions via CSRF attacks **CVE ID : CVE-2022-2245**		
Vendor: wpwax					
Product: directorist					
Affected Version(s): * Up to (excluding) 7.2.3					
Unrestricted Upload of File with Dangerous Type	08-Aug-2022	4.9	The Directorist WordPress plugin before 7.2.3 allows administrators to download other plugins from the same vendor directly to the site, but does not check the URL domain it gets the zip files from. This could allow administrators to run code on the server, which is a problem in multisite configurations. **CVE ID : CVE-2022-2046**	https://plugins.trac.wordpress.org/changeset/2752034/directorist?contextall=1&old=2731298&old_path=%2Fdirectorist	A-WPW-DIRE-170822/1563
Vendor: wpwhitesecurity					
Product: captcha_4wp					
Affected Version(s): * Up to (excluding) 7.1.0					
Cross-Site Request Forgery (CSRF)	01-Aug-2022	8.8	The CAPTCHA 4WP WordPress plugin before 7.1.0 lets user input reach a sensitive require_once call in one of its admin-side templates. This can be abused by attackers, via a	N/A	A-WPW-CAPT-170822/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cross-Site Request Forgery attack to run arbitrary code on the server. **CVE ID : CVE-2022-2184**		
Product: website_file_changes_monitor					
Affected Version(s): * Up to (excluding) 1.8.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Aug-2022	9.8	The Website File Changes Monitor WordPress plugin before 1.8.3 does not sanitise and escape user input before using it in a SQL statement via an action available to users with the manage_options capability (by default admins), leading to an SQL injection **CVE ID : CVE-2022-2269**	N/A	A-WPW-WEBS-170822/1565
Vendor: wpzoom					
Product: inspiro_pro					
Affected Version(s): * Up to (excluding) 7.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	5.4	The Inspiro PRO WordPress plugin does not sanitize the portfolio slider description, allowing users with privileges as low as Contributor to inject JavaScript into the description. **CVE ID : CVE-2022-2391**	N/A	A-WPZ-INSP-170822/1566
Vendor: wp_ds_blog_map_project					
Product: wp_ds_blog_map					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 3.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The WP DS Blog Map WordPress plugin through 3.1.3 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 when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2425**	N/A	A-WP_-WP_D-170822/1567
Vendor: wrteam					
Product: eshop_-_ecommerce_\/_store_website					
Affected Version(s): * Up to (including) 3.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	6.1	A Cross-site scripting (XSS) vulnerability in json search parse and the json response in wrteam.in, eShop - Multipurpose Ecommerce Store Website version 3.0.4 allows remote attackers to inject arbitrary web script or HTML via the get_products?search parameter. **CVE ID : CVE-2022-35493**	N/A	A-WRT-ESHO-170822/1568
Vendor: wsm_downloader_project					
Product: wsm_downloader					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.4.0					
Files or Directories Accessible to External Parties	08-Aug-2022	7.5	The WSM Downloader WordPress plugin through 1.4.0 allows any visitor to use its remote file download feature to download any local files, including sensitive ones like wp-config.php. **CVE ID : CVE-2022-2357**	N/A	A-WSM-WSM_-170822/1569
Authorization Bypass Through User-Controlled Key	08-Aug-2022	7.5	The WSM Downloader WordPress plugin through 1.4.0 allows only specific popular websites to download images/files from, this can be bypassed due to the lack of good "link" parameter validation **CVE ID : CVE-2022-2367**	N/A	A-WSM-WSM_-170822/1570
Vendor: xhyve_project					
Product: xhyve					
Affected Version(s): 0.2.0					
Stack-based Buffer Overflow	03-Aug-2022	6.7	This vulnerability allows local attackers to escalate privileges on affected installations of xhyve. An attacker must first obtain the ability to execute high-privileged code on the target guest	N/A	A-XHY-XHYV-170822/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system in order to exploit this vulnerability. The specific flaw exists within the e1000 virtual device. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-15056. **CVE ID : CVE-2022-35867**		
Vendor: yaycommerce					
Product: yaysmtp					
Affected Version(s): * Up to (excluding) 2.2.1					
Exposure of Resource to Wrong Sphere	01-Aug-2022	6.5	The YaySMTP WordPress plugin before 2.2.1 does not have capability check before displaying the Mailer Credentials in JS code for the settings, allowing any authenticated users, such as subscriber to retrieve them **CVE ID : CVE-2022-2370**	N/A	A-YAY-YAYS-170822/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	5.4	The YaySMTP WordPress plugin before 2.2.1 does not have proper authorisation when saving its settings, allowing users with a role as low as subscriber to change them, and use that to conduct Stored Cross-Site Scripting attack due to the lack of escaping in them as well. **CVE ID : CVE-2022-2371**	N/A	A-YAY-YAYS-170822/1573
Missing Authorization	01-Aug-2022	4.3	The YaySMTP WordPress plugin before 2.2.1 does not have capability check in an AJAX action, allowing any logged in users, such as subscriber to view the Logs of the plugin **CVE ID : CVE-2022-2369**	N/A	A-YAY-YAYS-170822/1574
Affected Version(s): * Up to (excluding) 2.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	4.8	The YaySMTP WordPress plugin before 2.2.2 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 when the unfiltered_html	N/A	A-YAY-YAYS-170822/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			capability is disallowed (for example in multisite setup) **CVE ID : CVE-2022-2372**		
Vendor: yop-poll					
Product: yop_poll					
Affected Version(s): * Up to (excluding) 6.4.3					
Authorization Bypass Through User-Controlled Key	01-Aug-2022	5.3	The YOP Poll WordPress plugin before 6.4.3 prioritizes getting a visitor's IP from certain HTTP headers over PHP's REMOTE_ADDR, which makes it possible to bypass IP-based limitations to vote in certain situations. **CVE ID : CVE-2022-1600**	N/A	A-YOP-YOP_-170822/1576
Vendor: Yuba					
Product: U5cms					
Affected Version(s): 8.3.5					
Cross-Site Request Forgery (CSRF)	03-Aug-2022	8.8	Yuba u5cms v8.3.5 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component savepage.php. This vulnerability allows attackers to execute arbitrary code. **CVE ID : CVE-2022-34937**	N/A	A-YUB-U5CM-170822/1577
Vendor: Zammad					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: Zammad					
Affected Version(s): 5.2.0					
Improper Restriction of Excessive Authentication Attempts	08-Aug-2022	9.8	Zammad 5.2.0 is vulnerable to privilege escalation. Zammad has a prevention against brute-force attacks trying to guess login credentials. After a configurable amount of attempts, users are invalidated and logins prevented. An attacker might work around this prevention, enabling them to send more than the configured amount of requests before the user invalidation takes place. **CVE ID : CVE-2022-35490**	https://zammad.com/de/advisories/zaa-2022-07	A-ZAM-ZAMM-170822/1578
Incorrect Authorization	08-Aug-2022	7.5	Zammad 5.2.0 suffers from Incorrect Access Control. Zammad did not correctly perform authorization on certain attachment endpoints. This could be abused by an unauthenticated attacker to gain access to attachments, such as emails or attached files.	https://zammad.com/de/advisories/zaa-2022-08	A-ZAM-ZAMM-170822/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35487		
Uncontrolled Resource Consumption	08-Aug-2022	7.5	In Zammad 5.2.0, an attacker could manipulate the rate limiting in the 'forgot password' feature of Zammad, and thereby send many requests for a known account to cause Denial Of Service by many generated emails which would also spam the victim. **CVE ID : CVE-2022-35488**	https://zammad.com/de/advisories/zaa-2022-05	A-ZAM-ZAMM-170822/1580
Incorrect Authorization	08-Aug-2022	6.5	In Zammad 5.2.0, customers who have secondary organizations assigned were able to see all organizations of the system rather than only those to which they are assigned. **CVE ID : CVE-2022-35489**	https://zammad.com/de/advisories/zaa-2022-06	A-ZAM-ZAMM-170822/1581
Vendor: Zlib					
Product: zlib					
Affected Version(s): * Up to (including) 1.2.12					
Out-of-bounds Write	05-Aug-2022	9.8	zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call	https://github.com/madler/zlib/commit/eff308af425b67093bab25f80f1ae950166bece1, http://www.openwall.com/lists/oss-	A-ZLI-ZLIB-170822/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference). **CVE ID : CVE-2022-37434**	security/2022/08/09/1	
Hardware					
Vendor: Airspan					
Product: airspot_5410					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Aug-2022	9.8	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a Unauthenticated remote command injection vulnerability. The ping functionality can be called without user authentication when crafting a malicious http request by injecting code in one of the parameters allowing for remote code execution. This vulnerability is exploited via the binary file /home/www/cgi-bin/diagnostics.cgi that accepts unauthenticated	N/A	H-AIR-AIRS-180822/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests and unsanitized data. As a result, a malicious actor can craft a specific request and interact remotely with the device. **CVE ID : CVE-2022-36267**		
Unrestricted Upload of File with Dangerous Type	08-Aug-2022	9.1	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists an Unauthenticated remote Arbitrary File Upload vulnerability which allows overwriting arbitrary files. A malicious actor can remotely upload a file of their choice and overwrite any file in the system by manipulating the filename and append a relative path that will be interpreted during the upload process. Using this method, it is possible to rewrite any file in the system or upload a new file. **CVE ID : CVE-2022-36264**	N/A	H-AIR-AIRS-180822/1584
N/A	08-Aug-2022	7.2	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a Hidden system command web page. After performing a reverse	N/A	H-AIR-AIRS-180822/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			engineering of the firmware, it was discovered that a hidden page not listed in the administration management interface allows a user to execute Linux commands on the device with root privileges. An authenticated malicious threat actor can use this page to fully compromise the device. **CVE ID : CVE-2022-36265**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	6.1	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a stored XSS vulnerability. As the binary file /home/www/cgi-bin/login.cgi does not check if the user is authenticated, a malicious actor can craft a specific request on the login.cgi endpoint that contains a base32 encoded XSS payload that will be accepted and stored. A successful attack will results in the injection of malicious scripts into the user settings page.	N/A	H-AIR-AIRS-180822/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-36266		
Vendor: Arris					
Product: bgw210					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**	N/A	H-ARR-BGW2-180822/1587
Product: bgw320					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the	N/A	H-ARR-BGW3-180822/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**		
Product: nvg443					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**	N/A	H-ARR-NVG4-180822/1589
Product: nvg510					
Affected Version(s): -					
Improper Limitation	04-Aug-2022	7.5	do_request in request.c in muhttpd	N/A	H-ARR-NVG5-180822/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**		
Product: nvg589					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and	N/A	H-ARR-NVG5-180822/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BGW320 devices are affected. **CVE ID : CVE-2022-31793**		
Product: nvg599					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**	N/A	H-ARR-NVG5-180822/1592
Vendor: Asus					
Product: et12					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin	N/A	H-ASU-ET12-180822/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: gt-ax11000					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-GT-A-180822/1594
Product: gt-ax11000_pro					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of	N/A	H-ASU-GT-A-180822/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: gt-ax6000					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-GT-A-180822/1596
Product: gt-axe16000					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists	N/A	H-ASU-GT-A-180822/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: rt-ax55					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-RT-A-180822/1598
Product: rt-ax56u					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-RT-A-180822/1599
Product: rt-ax58u					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-RT-A-180822/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rt-ax68u					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-RT-A-180822/1601
Product: rt-ax82u					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.	N/A	H-ASU-RT-A-180822/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26376		
Product: rt-ax86u					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-RT-A-180822/1603
Product: tuf-ax3000_v2					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to	N/A	H-ASU-TUF--180822/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: xd4					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-XD4-180822/1605
Product: xd6					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to	N/A	H-ASU-XD6-180822/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: xt12					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-XT12-180822/1607
Product: xt8					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to	N/A	H-ASU-XT8-180822/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: xt9					
Affected Version(s): -					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	H-ASU-XT9-180822/1609
Vendor: Cisco					
Product: asa_5506-x					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	H-CIS-ASA_-180822/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied	rsa-key-leak-Ms7UEfZz	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: asa_5506h-x					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-ASA_-180822/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: asa_5506w-x					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-ASA_-180822/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: asa_5508-x					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-ASA_-180822/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: asa_5516-x					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-ASA_-180822/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_1000					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_1010					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_1020					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis	H-CIS-FIRE-180822/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical	co-sa-asaftd-rsa-key-leak-Ms7UEfZz	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_1030					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_1040					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_1120					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_1140					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: firepower_1150					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_2100					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_2110					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_2120					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_2130					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	H-CIS-FIRE-180822/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied	rsa-key-leak-Ms7UEfZz	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_2140					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4100					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4110					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4112					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4115					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4120					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4125					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis	H-CIS-FIRE-180822/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical	co-sa-asaftd-rsa-key-leak-Ms7UEfZz	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4140					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4145					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_4150					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: firepower_9300					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-FIRE-180822/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rv160					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV16-180822/1638
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV16-180822/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv160w					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV16-180822/1640
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV16-180822/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv260					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV26-180822/1642
Improper Neutralization of Special Elements used in an OS Command ('OS	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV26-180822/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv260p					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV26-180822/1644
Improper Neutralization of Special Elements used in an	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-	H-CIS-RV26-180822/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	vuln-CbVp4SUR	
Product: rv260w					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV26-180822/1646
Improper Neutralizat	10-Aug-2022	10	Multiple vulnerabilities in	https://tools.cisco.com/securi	H-CIS-RV26-180822/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	
Product: rv340					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20842		
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1649
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv340w					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20842**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1651
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1653
Product: rv345					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20842**		
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1655
Improper Neutralization of Special Elements used in an OS Command ('OS	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv345p					
Affected Version(s): -					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20842**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1657
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cis	H-CIS-RV34-180822/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	co-sa-sb-mult-vuln-CbVp4SUR	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	H-CIS-RV34-180822/1659
Product: secure_firewall_3110					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-SECU-180822/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: secure_firewall_3120					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-SECU-180822/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: secure_firewall_3130					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-	H-CIS-SECU-180822/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied	rsa-key-leak-Ms7UEfZz	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Product: secure_firewall_3140					
Affected Version(s): -					
Observable Discrepancy	10-Aug-2022	7.5	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz	H-CIS-SECU-180822/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. **CVE ID : CVE-2022-20866**		
Vendor: Dlink					
Product: dir-818l					
Affected Version(s): -					
N/A	03-Aug-2022	9.8	D-LINK DIR-818LW A1:DIR818L_FW105 b01 was discovered to contain a remote code execution (RCE) vulnerability via the function ssdpcgi_main. **CVE ID : CVE-2022-35619**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--180822/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	03-Aug-2022	9.8	D-LINK DIR-818LW A1:DIR818L_FW105 b01 was discovered to contain a remote code execution (RCE) vulnerability via the function binary.soapcgi_main. **CVE ID : CVE-2022-35620**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--180822/1665
Product: dir820la1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2022	9.8	D-Link DIR810LA1_FW102B22 was discovered to contain a command injection vulnerability via the Ping_addr function. **CVE ID : CVE-2022-34974**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR8-180822/1666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2022	7.5	D-Link DIR820LA1_FW106B02 was discovered to contain a buffer overflow via the nextPage parameter at ping.ccp. **CVE ID : CVE-2022-34973**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR8-180822/1667
Vendor: IBM					
Product: mq_appliance_m2001					
Affected Version(s): -					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node	H-IBM-MQ_A-180822/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	
Product: mq_appliance_m2002					
Affected Version(s): -					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	H-IBM-MQ_A-180822/1669
Vendor: mediatek					
Product: mt2621					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	9.8	In httpclient, there is a possible out of bounds write due to uninitialized data. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT26-180822/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: WSAP00103831; Issue ID: WSAP00103831. **CVE ID : CVE-2022-26437**		
Product: mt2625					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	9.8	In httpclient, there is a possible out of bounds write due to uninitialized data. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WSAP00103831; Issue ID: WSAP00103831. **CVE ID : CVE-2022-26437**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT26-180822/1671
Product: mt6580					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT65-180822/1672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Product: mt6735					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1673
Product: mt6739					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1675
Product: mt6757					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26429		
Product: mt6761					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1677
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1678
Product: mt6762					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1679
Product: mt6763					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt6765					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1681
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1682
Product: mt6768					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1683
Product: mt6769					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1684
Product: mt6771					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1685
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1686
Product: mt6779					
Affected Version(s): -					
Incorrect Default	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage	https://corp.mediatek.com/product-security-	H-MED-MT67-180822/1687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	bulletin/August-2022	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1688
Product: mt6781					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1690
Product: mt6785					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT67-180822/1692
Product: mt6833					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1694
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085540; Issue ID: ALPS07085540. **CVE ID : CVE-2022-26427**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1696
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1697
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, 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/August-2022	H-MED-MT68-180822/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1699
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1701
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1702
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-180822/1703

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: ALPS06479306; Issue ID: ALPS06479306. **CVE ID : CVE-2022-21790**	bulletin/August-2022	
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1704
Product: mt6853					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1706
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085540; Issue ID: ALPS07085540. **CVE ID : CVE-2022-26427**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1708
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1710
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1711
Access of Resource Using Incompatible Type	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1713
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1715
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06479306; Issue ID: ALPS06479306. **CVE ID : CVE-2022-21790**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1716
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-180822/1717

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: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**	bulletin/August-2022	
Product: mt6853t					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1718
Concurrent Execution using Shared Resource with Improper	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1719

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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**		
Product: mt6855					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1720
Out-of-bounds Read	01-Aug-2022	4.4	In emi mpu, 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/August-2022	H-MED-MT68-180822/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07023666; Issue ID: ALPS07023666. **CVE ID : CVE-2022-26436**		
Product: mt6873					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1722
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1724
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085540; Issue ID: ALPS07085540. **CVE ID : CVE-2022-26427**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1726
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1727
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, 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/August-2022	H-MED-MT68-180822/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1729
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1731
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1732
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT68-180822/1733

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: ALPS06479306; Issue ID: ALPS06479306. **CVE ID : CVE-2022-21790**	bulletin/August-2022	
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1734
Product: mt6875					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1736
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**		
Product: mt6877					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1738
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410; Issue ID: ALPS07085410.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21792		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1740
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085540; Issue ID: ALPS07085540. **CVE ID : CVE-2022-26427**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1741
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This	https://corp.mediatek.com/product-security-	H-MED-MT68-180822/1742

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: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1743
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due 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/August-2022	H-MED-MT68-180822/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1745
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1747
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1748
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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/August-2022	H-MED-MT68-180822/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06479306; Issue ID: ALPS06479306. **CVE ID : CVE-2022-21790**		
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1750
Product: mt6879					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
N/A	01-Aug-2022	6.7	In scp, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06988728; Issue ID: ALPS06988728. **CVE ID : CVE-2022-21788**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1752
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1754
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1755
Access of Resource Using Incompatible Type	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1757
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1759
Out-of-bounds Read	01-Aug-2022	4.4	In emi mpu, 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: ALPS07023666; Issue ID: ALPS07023666. **CVE ID : CVE-2022-26436**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1760
Product: mt6883					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1761
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1762
Concurrent Execution using Shared Resource with	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption due to a race condition. This could lead to local escalation of	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**		
Product: mt6885					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1764
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1766
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26431		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1768
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1769
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1770

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: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1771
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**		
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1773
Product: mt6889					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26429		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1775
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1776
Product: mt6891					
Affected Version(s): -					
Concurrent Execution using	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption due to a	https://corp.mediatek.com/product-security-	H-MED-MT68-180822/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	bulletin/August-2022	
Product: mt6893					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1778
Out-of-bounds Write	01-Aug-2022	6.7	In camera isp, 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/August-2022	H-MED-MT68-180822/1779

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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1780
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085540;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07085540. **CVE ID : CVE-2022-26427**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1782
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1783
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to	https://corp.mediatek.com/product-security-	H-MED-MT68-180822/1784

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: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	bulletin/August-2022	
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1785
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of 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/August-2022	H-MED-MT68-180822/1786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1787
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06479306; Issue ID: ALPS06479306. **CVE ID : CVE-2022-21790**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1789
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1790
Product: mt6895					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app	https://corp.mediatek.com/product-security-	H-MED-MT68-180822/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	bulletin/August-2022	
N/A	01-Aug-2022	6.7	In scp, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06988728; Issue ID: ALPS06988728. **CVE ID : CVE-2022-21788**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1792
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1794
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26432		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1796
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1797
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1798

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: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1799
Out-of-bounds Read	01-Aug-2022	4.4	In emi mpu, 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: ALPS07023666;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT68-180822/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07023666. **CVE ID : CVE-2022-26436**		
Product: mt6983					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1801
N/A	01-Aug-2022	6.7	In scp, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06988728; Issue ID: ALPS06988728.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-21788		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1803
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1804
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1805

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: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1806
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a 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/August-2022	H-MED-MT69-180822/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1808
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1809
Out-of-bounds Read	01-Aug-2022	4.4	In emi mpu, there is a possible out of bounds read due to a	https://corp.mediatek.com/product-security-	H-MED-MT69-180822/1810

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: ALPS07023666; Issue ID: ALPS07023666. **CVE ID : CVE-2022-26436**	bulletin/August-2022	
Product: mt6985					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT69-180822/1811
Product: mt7603					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1812

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: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1813
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due 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/August-2022	H-MED-MT76-180822/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1815
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1817
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1818
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1819

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: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**		
Product: mt7610					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1820
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	H-MED-MT76-180822/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1822
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26441		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1824
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1825
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT76-180822/1826

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: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1827
Product: mt7612					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1829
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1831
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1833
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1834
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1835

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: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**		
Product: mt7613					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1836
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	H-MED-MT76-180822/1837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1838
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26441		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1840
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1841
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT76-180822/1842

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: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1843
Product: mt7615					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1845
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1847
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1849
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1850
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1851

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: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**		
Product: mt7620					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1852
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	H-MED-MT76-180822/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1854
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26441		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1856
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1857
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT76-180822/1858

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: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1859
Product: mt7622					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1861
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1863
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1865
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1866
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1867

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: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**		
Product: mt7628					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1868
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	H-MED-MT76-180822/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1870
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26441		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1872
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1873
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT76-180822/1874

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: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1875
Product: mt7629					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1877
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1879
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1881
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT76-180822/1882
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT76-180822/1883

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: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**		
Product: mt7915					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1884
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	H-MED-MT79-180822/1885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1886
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26441		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1888
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1889
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT79-180822/1890

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: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1891
Product: mt7916					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT79-180822/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1893
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1895
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1897
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1898
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	H-MED-MT79-180822/1899

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: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**		
Product: mt7986					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1900
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	H-MED-MT79-180822/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1902
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26441		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1904
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1905
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT79-180822/1906

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: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT79-180822/1907
Product: mt8163					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchroniz	01-Aug-2022	6.4	In video codec, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ation ('Race Condition')			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**		
Product: mt8167					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1909
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1911
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1912
Concurrent Execution using	01-Aug-2022	6.4	In video codec, there is a possible memory corruption due to a	https://corp.mediatek.com/product-security-	H-MED-MT81-180822/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	bulletin/August-2022	
Product: mt8167s					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1914
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1916
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26435		
Product: mt8168					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1918
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1920
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1921
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Product: mt8173					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1923
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. 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/August-2022	H-MED-MT81-180822/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1925
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1926
Concurrent Execution	01-Aug-2022	6.4	In video codec, there is a possible memory	https://corp.mediatek.com/pr	H-MED-MT81-180822/1927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	oduct-security-bulletin/August-2022	
Product: mt8175					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1928
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1930
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Product: mt8183					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1932
Product: mt8185					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1934
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1935
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to	https://corp.mediatek.com/product-security-	H-MED-MT81-180822/1936

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: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1937
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1939
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT81-180822/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt8321					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1941
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1942
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT83-180822/1943

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: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1944
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. 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/August-2022	H-MED-MT83-180822/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1946
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1947
Product: mt8362a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1948
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1949
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, 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/August-2022	H-MED-MT83-180822/1950

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: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1951
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**		
Product: mt8365					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1953
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26426		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1955
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1956
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1957

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: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Product: mt8385					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1958
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1960
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26431		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1962
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1963
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1964

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: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1965
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT83-180822/1966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**		
Product: mt8532					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT85-180822/1967
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT85-180822/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT85-180822/1969
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT85-180822/1970
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, 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/August-2022	H-MED-MT85-180822/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT85-180822/1972
Product: mt8666					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1974
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1976
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1977
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, 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/August-2022	H-MED-MT86-180822/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1979
Product: mt8675					
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1981
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1983
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1984
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, 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/August-2022	H-MED-MT86-180822/1985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1986
Product: mt8695					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT86-180822/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**		
Product: mt8765					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1988
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26426		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1990
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1991
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1992

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: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1993
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a 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/August-2022	H-MED-MT87-180822/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1995
Product: mt8766					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26429		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1997
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1998
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/1999

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: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2000
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a 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/August-2022	H-MED-MT87-180822/2001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2002
Product: mt8768					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26429		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2004
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2005
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2006

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: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2007
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a 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/August-2022	H-MED-MT87-180822/2008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2009
Product: mt8786					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415.	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26429		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2011
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2012
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2013

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: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2014
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. 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/August-2022	H-MED-MT87-180822/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2016
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2017
Product: mt8788					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2018
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2019
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This	https://corp.mediatek.com/product-security-	H-MED-MT87-180822/2020

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: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2021
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due 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/August-2022	H-MED-MT87-180822/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2023
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2025
Product: mt8789					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2026
Out-of-bounds Write	01-Aug-2022	6.7	In camera isp, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	H-MED-MT87-180822/2027

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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2028
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due 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/August-2022	H-MED-MT87-180822/2029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2030
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2032
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2033
Product: mt8791					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2035
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. 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/August-2022	H-MED-MT87-180822/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2037
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2039
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2040
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2042
Product: mt8797					
Affected Version(s): -					
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07025415; Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2044
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2046
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2047
Access of Resource Using Incompatible Type	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2049
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435;	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2051
Product: mt8798					
Affected Version(s): -					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT87-180822/2052
Product: mt8981					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT89-180822/2053
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT89-180822/2054
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT89-180822/2055

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT89-180822/2056
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due 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/August-2022	H-MED-MT89-180822/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT89-180822/2058
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT89-180822/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	H-MED-MT89-180822/2060
Vendor: megatech					
Product: msnswitch					
Affected Version(s): -					
Improper Authentication	10-Aug-2022	9.8	An authentication-bypass issue in the component http://MYDEVICEIP/cgi-bin-sdb/ExportSettings.sh of Mega System Technologies Inc MSNSwitch MNT.2408 allows unauthenticated attackers to arbitrarily configure settings within the application, leading to remote code execution. **CVE ID : CVE-2022-32429**	N/A	H-MEG-MSNS-180822/2061
Vendor: Realtek					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ecos_msdk					
Affected Version(s): -					
Improper Input Validation	01-Aug-2022	9.8	In Realtek eCos RSDK 1.5.7p1 and MSDK 4.9.4p1, the SIP ALG function that rewrites SDP data has a stack-based buffer overflow. This allows an attacker to remotely execute code without authentication via a crafted SIP packet that contains malicious SDP data. **CVE ID : CVE-2022-27255**	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2022-27255.pdf	H-REA-ECOS-180822/2062
Product: ecos_rsdk					
Affected Version(s): -					
Improper Input Validation	01-Aug-2022	9.8	In Realtek eCos RSDK 1.5.7p1 and MSDK 4.9.4p1, the SIP ALG function that rewrites SDP data has a stack-based buffer overflow. This allows an attacker to remotely execute code without authentication via a crafted SIP packet that contains malicious SDP data. **CVE ID : CVE-2022-27255**	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2022-27255.pdf	H-REA-ECOS-180822/2063
Vendor: Samsung					
Product: charm					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.5	PendingIntent hijacking vulnerability in releaseAlarm in Charm by Samsung prior to version 1.2.3 allows local attackers to access files without permission via implicit intent. **CVE ID : CVE-2022-36829**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	H-SAM-CHAR-180822/2064
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.5	PendingIntent hijacking vulnerability in cancelAlarmManager in Charm by Samsung prior to version 1.2.3 allows local attackers to access files without permission via implicit intent. **CVE ID : CVE-2022-36830**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	H-SAM-CHAR-180822/2065
Missing Authorization	05-Aug-2022	5.5	Unprotected provider vulnerability in Charm by Samsung prior to version 1.2.3 allows attackers to read connection state without permission. **CVE ID : CVE-2022-36836**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	H-SAM-CHAR-180822/2066
Vendor: tcl					
Product: linkhub_mesh_wifi_ac1200					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2022	9.8	An os command injection vulnerability exists in the confsrv ucloud_add_new_node functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to arbitrary command execution. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-21178**	N/A	H-TCL-LINK-180822/2067
N/A	05-Aug-2022	9.8	A denial of service vulnerability exists in the confctl_set_wan_cfg functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27178**	N/A	H-TCL-LINK-180822/2068
Improper Neutralization of Special Elements used in an OS Command ('OS	05-Aug-2022	9.8	An os command injection vulnerability exists in the confsrv ucloud_add_node functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted	N/A	H-TCL-LINK-180822/2069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			network packet can lead to arbitrary command execution. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-22140**		
Use of Hard-coded Credentials	05-Aug-2022	9.8	A hard-coded password vulnerability exists in the libcommonprod.so prod_change_root_passwd functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. During system startup this functionality is always called, leading to a known root password. An attacker does not have to do anything to trigger this vulnerability. **CVE ID : CVE-2022-22144**	N/A	H-TCL-LINK-180822/2070
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv confctl_set_app_language functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based	N/A	H-TCL-LINK-180822/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-23103**		
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv set_port_fwd_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-23399**	N/A	H-TCL-LINK-180822/2072
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv set_mf_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.This vulnerability leverages the	N/A	H-TCL-LINK-180822/2073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ethAddr field within the protobuf message to cause a buffer overflow. **CVE ID : CVE-2022-23918**		
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv set_mf_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.This vulnerability leverages the name field within the protobuf message to cause a buffer overflow. **CVE ID : CVE-2022-23919**	N/A	H-TCL-LINK-180822/2074
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this	N/A	H-TCL-LINK-180822/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the ap_steer binary. **CVE ID : CVE-2022-24005**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the arpbrocast binary. **CVE ID : CVE-2022-24006**	N/A	H-TCL-LINK-180822/2076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify	N/A	H-TCL-LINK-180822/2077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the cfm binary. **CVE ID : CVE-2022-24007**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the confcli binary. **CVE ID : CVE-2022-24008**	N/A	H-TCL-LINK-180822/2078
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An	N/A	H-TCL-LINK-180822/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the confsrv binary. **CVE ID : CVE-2022-24009**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the cwmpd binary. **CVE ID : CVE-2022-24010**	N/A	H-TCL-LINK-180822/2080
Buffer Copy without Checking Size of Input ('Classic	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer	N/A	H-TCL-LINK-180822/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the device_list binary. **CVE ID : CVE-2022-24011**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the fota binary. **CVE ID : CVE-2022-24012**	N/A	H-TCL-LINK-180822/2082
Buffer Copy without Checking Size of Input ('Classic	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted	N/A	H-TCL-LINK-180822/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the gpio_ctrl binary. **CVE ID : CVE-2022-24013**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the logserver binary. **CVE ID : CVE-2022-24014**	N/A	H-TCL-LINK-180822/2084
Buffer Copy without Checking Size of Input	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14.	N/A	H-TCL-LINK-180822/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the log_upload binary. **CVE ID : CVE-2022-24015**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the mesh_status_check binary. **CVE ID : CVE-2022-24016**	N/A	H-TCL-LINK-180822/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the miniupnpd binary. **CVE ID : CVE-2022-24017**	N/A	H-TCL-LINK-180822/2087
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within	N/A	H-TCL-LINK-180822/2088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the multiWAN binary. **CVE ID : CVE-2022-24018**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the netctrl binary. **CVE ID : CVE-2022-24019**	N/A	H-TCL-LINK-180822/2089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the	N/A	H-TCL-LINK-180822/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow vulnerability within the network_check binary. **CVE ID : CVE-2022-24020**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the online_process binary. **CVE ID : CVE-2022-24021**	N/A	H-TCL-LINK-180822/2091
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This	N/A	H-TCL-LINK-180822/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability represents all occurances of the buffer overflow vulnerability within the pannn binary. **CVE ID : CVE-2022-24022**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the rtk_ate binary. **CVE ID : CVE-2022-24024**	N/A	H-TCL-LINK-180822/2093
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this	N/A	H-TCL-LINK-180822/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the sntp binary. **CVE ID : CVE-2022-24025**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the telnet_ate_monitor binary. **CVE ID : CVE-2022-24026**	N/A	H-TCL-LINK-180822/2095
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An	N/A	H-TCL-LINK-180822/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the libcommon.so binary. **CVE ID : CVE-2022-24027**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the libcommonprod.so binary. **CVE ID : CVE-2022-24028**	N/A	H-TCL-LINK-180822/2097
Buffer Copy without Checking Size of Input	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14.	N/A	H-TCL-LINK-180822/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the rp-pppoe.so binary. **CVE ID : CVE-2022-24029**		
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv addTimeGroup functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-25996**	N/A	H-TCL-LINK-180822/2099
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv ucloud_set_node_location functionality of TCL LinkHub Mesh Wi-Fi	N/A	H-TCL-LINK-180822/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-26009**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the confsrv ucloud_set_node_location functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-26342**	N/A	H-TCL-LINK-180822/2101
N/A	05-Aug-2022	9.8	A denial of service vulnerability exists in the ucloud_del_node functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to	N/A	H-TCL-LINK-180822/2102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger this vulnerability. **CVE ID : CVE-2022-26346**		
Out-of-bounds Write	05-Aug-2022	8.8	A stack-based buffer overflow vulnerability exists in the confers ucloud_add_node_new functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-21201**	N/A	H-TCL-LINK-180822/2103
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	8.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow	N/A	H-TCL-LINK-180822/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability within the pppd binary. **CVE ID : CVE-2022-24023**		
N/A	05-Aug-2022	7.5	A denial of service vulnerability exists in the confctl_set_master_wlan functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27185**	N/A	H-TCL-LINK-180822/2105
Exposure of Sensitive Information to an Unauthorized Actor	05-Aug-2022	7.5	An information disclosure vulnerability exists in the confctl_get_master_wlan functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to information disclosure. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27630**	N/A	H-TCL-LINK-180822/2106
Exposure of Sensitive Informatio	05-Aug-2022	7.5	An information disclosure vulnerability exists	N/A	H-TCL-LINK-180822/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to an Unauthorized Actor			in the confctl_get_guest_wlan functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to information disclosure. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27633**		
Improper Access Control	05-Aug-2022	7.5	A denial of service vulnerability exists in the confctl_set_guest_wlan functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27660**	N/A	H-TCL-LINK-180822/2108
Vendor: tem					
Product: flex-1085					
Affected Version(s): -					
Improper Resource Shutdown or Release	01-Aug-2022	7.5	A vulnerability classified as critical has been found in TEM FLEX-1085 1.6.0. Affected is an unknown function of the file	N/A	H-TEM-FLEX-180822/2109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/sistema/flash/reboot. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2591**		
Vendor: totolink					
Product: a3002ru					
Affected Version(s): -					
Use of Hard-coded Credentials	10-Aug-2022	9.8	TOTOLINK A3002RU V3.0.0-B20220304.1804 has a hardcoded password for root in /etc/shadow.sample. **CVE ID : CVE-2022-35491**	N/A	H-TOT-A300-180822/2110
Product: a3600r					
Affected Version(s): -					
Use of Hard-coded Credentials	04-Aug-2022	9.8	Totolink A3600R_Firmware V4.1.2cu.5182_B20201102 contains a hard code password for root in /etc/shadow.sample. **CVE ID : CVE-2022-34993**	http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=63&ids=36image-20220606105532193	H-TOT-A360-180822/2111
Vendor: unitree					
Product: go_1					
Affected Version(s): h0.1.7					
Improper Authentication	05-Aug-2022	6.5	Using off-the-shelf commodity hardware, the	N/A	H-UNI-GO_1-180822/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Unitree Go 1 robotics platform version H0.1.7 and H0.1.9 (using firmware version 0.1.35) can be powered down by an attacker within normal RF range without authentication. Other versions may be affected, such as the A1. **CVE ID : CVE-2022-2675**		
Affected Version(s): h0.1.9					
Improper Authentication	05-Aug-2022	6.5	Using off-the-shelf commodity hardware, the Unitree Go 1 robotics platform version H0.1.7 and H0.1.9 (using firmware version 0.1.35) can be powered down by an attacker within normal RF range without authentication. Other versions may be affected, such as the A1. **CVE ID : CVE-2022-2675**	N/A	H-UNI-GO_1-180822/2113
Vendor: wavlink					
Product: wn530h4					
Affected Version(s): -					
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	H-WAV-WN53-180822/2114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	H-WAV-WN53-180822/2115
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml.	N/A	H-WAV-WN53-180822/2116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35520		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**	N/A	H-WAV-WN53-180822/2117
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	H-WAV-WN53-180822/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**	N/A	H-WAV-WN53-180822/2119
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**	N/A	H-WAV-WN53-180822/2120
Improper Neutralization of Special Elements used in a Command	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on	N/A	H-WAV-WN53-180822/2121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	H-WAV-WN53-180822/2122
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**	N/A	H-WAV-WN53-180822/2123
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on	N/A	H-WAV-WN53-180822/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	H-WAV-WN53-180822/2125
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	H-WAV-WN53-180822/2126
Improper Neutralization of	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8,	N/A	H-WAV-WN53-180822/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**	N/A	H-WAV-WN53-180822/2128
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid,	N/A	H-WAV-WN53-180822/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**		
Product: wn531p3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**	N/A	H-WAV-WN53-180822/2130
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml.	N/A	H-WAV-WN53-180822/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35519		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**	N/A	H-WAV-WN53-180822/2132
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**	N/A	H-WAV-WN53-180822/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	H-WAV-WN53-180822/2134
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**	N/A	H-WAV-WN53-180822/2135
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal,	N/A	H-WAV-WN53-180822/2136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**	N/A	H-WAV-WN53-180822/2137
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	H-WAV-WN53-180822/2138
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	H-WAV-WN53-180822/2139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**	N/A	H-WAV-WN53-180822/2140
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	H-WAV-WN53-180822/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	H-WAV-WN53-180822/2142
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**	N/A	H-WAV-WN53-180822/2143
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and	N/A	H-WAV-WN53-180822/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**	N/A	H-WAV-WN53-180822/2145
Product: wn533a8					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to	N/A	H-WAV-WN53-180822/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	H-WAV-WN53-180822/2147
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**	N/A	H-WAV-WN53-180822/2148
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	H-WAV-WN53-180822/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	H-WAV-WN53-180822/2150
Improper Neutralization of Special Elements used in a Command	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no	N/A	H-WAV-WN53-180822/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**	N/A	H-WAV-WN53-180822/2152
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml.	N/A	H-WAV-WN53-180822/2153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35525		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	H-WAV-WN53-180822/2154
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**	N/A	H-WAV-WN53-180822/2155
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page	N/A	H-WAV-WN53-180822/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	H-WAV-WN53-180822/2157
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	H-WAV-WN53-180822/2158
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on	N/A	H-WAV-WN53-180822/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**	N/A	H-WAV-WN53-180822/2160
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and	N/A	H-WAV-WN53-180822/2161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**		
Product: wn535g3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**	N/A	H-WAV-WN53-180822/2162
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	H-WAV-WN53-180822/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**	N/A	H-WAV-WN53-180822/2164
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**	N/A	H-WAV-WN53-180822/2165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	H-WAV-WN53-180822/2166
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**	N/A	H-WAV-WN53-180822/2167
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal,	N/A	H-WAV-WN53-180822/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**	N/A	H-WAV-WN53-180822/2169
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	H-WAV-WN53-180822/2170
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	H-WAV-WN53-180822/2171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**	N/A	H-WAV-WN53-180822/2172
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	H-WAV-WN53-180822/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	H-WAV-WN53-180822/2174
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**	N/A	H-WAV-WN53-180822/2175
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and	N/A	H-WAV-WN53-180822/2176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**	N/A	H-WAV-WN53-180822/2177
Product: wn572hp3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to	N/A	H-WAV-WN57-180822/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	H-WAV-WN57-180822/2179
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**	N/A	H-WAV-WN57-180822/2180
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	H-WAV-WN57-180822/2181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	H-WAV-WN57-180822/2182
Improper Neutralization of Special Elements used in a Command	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no	N/A	H-WAV-WN57-180822/2183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**	N/A	H-WAV-WN57-180822/2184
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml.	N/A	H-WAV-WN57-180822/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35525		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	H-WAV-WN57-180822/2186
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**	N/A	H-WAV-WN57-180822/2187
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page	N/A	H-WAV-WN57-180822/2188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	H-WAV-WN57-180822/2189
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	H-WAV-WN57-180822/2190
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on	N/A	H-WAV-WN57-180822/2191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**	N/A	H-WAV-WN57-180822/2192
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and	N/A	H-WAV-WN57-180822/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**		
Operating System					
Vendor: Airspan					
Product: airspot_5410_firmware					
Affected Version(s): * Up to (including) 0.3.4.1-4					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	08-Aug-2022	9.8	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a Unauthenticated remote command injection vulnerability. The ping functionality can be called without user authentication when crafting a malicious http request by injecting code in one of the parameters allowing for remote code execution. This vulnerability is exploited via the binary file /home/www/cgi-bin/diagnostics.cgi that accepts unauthenticated requests and unsanitized data. As a result, a malicious actor can craft a specific request and	N/A	O-AIR-AIRS-180822/2194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interact remotely with the device. **CVE ID : CVE-2022-36267**		
Unrestricted Upload of File with Dangerous Type	08-Aug-2022	9.1	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists an Unauthenticated remote Arbitrary File Upload vulnerability which allows overwriting arbitrary files. A malicious actor can remotely upload a file of their choice and overwrite any file in the system by manipulating the filename and append a relative path that will be interpreted during the upload process. Using this method, it is possible to rewrite any file in the system or upload a new file. **CVE ID : CVE-2022-36264**	N/A	O-AIR-AIRS-180822/2195
N/A	08-Aug-2022	7.2	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a Hidden system command web page. After performing a reverse engineering of the firmware, it was discovered that a hidden page not listed in the	N/A	O-AIR-AIRS-180822/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administration management interface allows a user to execute Linux commands on the device with root privileges. An authenticated malicious threat actor can use this page to fully compromise the device. **CVE ID : CVE-2022-36265**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-2022	6.1	In Airspan AirSpot 5410 version 0.3.4.1-4 and under there exists a stored XSS vulnerability. As the binary file /home/www/cgi-bin/login.cgi does not check if the user is authenticated, a malicious actor can craft a specific request on the login.cgi endpoint that contains a base32 encoded XSS payload that will be accepted and stored. A successful attack will results in the injection of malicious scripts into the user settings page. **CVE ID : CVE-2022-36266**	N/A	O-AIR-AIRS-180822/2197
Vendor: Apple					
Product: macos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Uncontrolled Search Path Element	11-Aug-2022	7.8	Adobe Premiere Elements version 2020v20 (and earlier) is affected by an Uncontrolled Search Path Element which could lead to Privilege Escalation. An attacker could leverage this vulnerability to obtain admin using an existing low-privileged user. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-34235**	https://helpx.adobe.com/security/products/premiere_elements/apsb22-43.html	O-APP-MACO-180822/2198
Out-of-bounds Write	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34260**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	O-APP-MACO-180822/2199
Use After Free	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and	https://helpx.adobe.com/secu	O-APP-MACO-180822/2200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 25.4.6 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34263**	rity/products/illustrator/apsb22-41.html	
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28880**	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	O-APP-MACO-180822/2201
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/sec	O-APP-MACO-180822/2202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	urity-advisories	
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34261**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	O-APP-MACO-180822/2203
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	O-APP-MACO-180822/2204

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-2022-34262**		
Vendor: Arris					
Product: bgw210_firmware					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**	N/A	O-ARR-BGW2-180822/2205
Product: bgw320_firmware					
Affected Version(s): -					
Improper Limitation of a Pathname to a	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files	N/A	O-ARR-BGW3-180822/2206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**		
Product: nvg443_firmware					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected.	N/A	O-ARR-NVG4-180822/2207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-31793		
Product: nvg510_firmware					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**	N/A	O-ARR-NVG5-180822/2208
Product: nvg589_firmware					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when	N/A	O-ARR-NVG5-180822/2209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**		
Product: nvg599_firmware					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	04-Aug-2022	7.5	do_request in request.c in muhttpd before 1.1.7 allows remote attackers to read arbitrary files by constructing a URL with a single character before a desired path on the filesystem. This occurs because the code skips over the first character when serving files. Arris NVG443, NVG599, NVG589, and NVG510 devices and Arris-derived BGW210 and BGW320 devices are affected. **CVE ID : CVE-2022-31793**	N/A	O-ARR-NVG5-180822/2210
Vendor: Asus					
Product: asuswrt					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48706					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists	N/A	O-ASU-ASUS-180822/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: et12_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48823					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-ET12-180822/2212
Product: gt-ax11000_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_49559					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-GT-A-180822/2213
Product: gt-ax11000_pro_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48996					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-GT-A-180822/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gt-ax6000_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48823					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-GT-A-180822/2215
Product: gt-axe16000_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48786					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.	N/A	O-ASU-GT-A-180822/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26376		
Product: rt-ax55_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_49559					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-RT-A-180822/2217
Product: rt-ax56u_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_49559					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to	N/A	O-ASU-RT-A-180822/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: rt-ax58u_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48908					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-RT-A-180822/2219
Product: rt-ax68u_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_49479					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to	N/A	O-ASU-RT-A-180822/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: rt-ax82u_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_49380					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-RT-A-180822/2221
Product: rt-ax86u_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_49447					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to	N/A	O-ASU-RT-A-180822/2222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: tuf-ax3000_v2_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48750					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-TUF--180822/2223
Product: xd4_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48790					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to	N/A	O-ASU-XD4_-180822/2224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: xd6_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_49356					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-XD6_-180822/2225
Product: xt12_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48823					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd	N/A	O-ASU-XT12-180822/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**		
Product: xt8_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.386_48706					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-XT8_-180822/2227
Product: xt9_firmware					
Affected Version(s): * Up to (excluding) 3.0.0.4.388_20027					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-26376**	N/A	O-ASU-XT9_-180822/2228
Vendor: asuswrt-merlin					
Product: new_gen					
Affected Version(s): * Up to (excluding) 386.7					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of Asuswrt prior to 3.0.0.4.386_48706 and Asuswrt-Merlin New Gen prior to 386.7.. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.	N/A	O-ASU-NEW_-180822/2229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26376		
Vendor: bosch					
Product: bf-os					
Affected Version(s): From (including) 3.0 Up to (including) 3.83					
Weak Password Requirements	01-Aug-2022	7.5	BF-OS version 3.x up to and including 3.83 do not enforce strong passwords which may allow a remote attacker to brute-force the device password. **CVE ID : CVE-2022-36301**	https://psirt.bosch.com/security-advisories/bosch-sa-013924-bt.html	O-BOS-BF-O-180822/2230
Affected Version(s): From (including) 3.00 Up to (including) 3.83					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Aug-2022	5.4	File path manipulation vulnerability in BF-OS version 3.00 up to and including 3.83 allows an attacker to modify the file path to access different resources, which may contain sensitive information. **CVE ID : CVE-2022-36302**	https://psirt.bosch.com/security-advisories/bosch-sa-013924-bt.html	O-BOS-BF-O-180822/2231
Vendor: Canonical					
Product: ubuntu_linux					
Affected Version(s): 16.04					
N/A	10-Aug-2022	6.5	Linux deployments of StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.2 deployed	https://security.netapp.com/advisory/NTAP-20220808-0001/	O-CAN-UBUN-180822/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with a Linux kernel version less than 4.7.0 are susceptible to a vulnerability which could allow a remote unauthenticated attacker to view limited metrics information and modify alert email recipients and content. **CVE ID : CVE-2022-23238**		
Vendor: Centos					
Product: centos					
Affected Version(s): 7.9					
N/A	10-Aug-2022	6.5	Linux deployments of StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.2 deployed with a Linux kernel version less than 4.7.0 are susceptible to a vulnerability which could allow a remote unauthenticated attacker to view limited metrics information and modify alert email recipients and content. **CVE ID : CVE-2022-23238**	https://security.netapp.com/advisory/NTAP-20220808-0001/	O-CEN-CENT-180822/2233
Vendor: Cisco					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: rv160w_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.05					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV16-180822/2234
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV16-180822/2235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv160_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.05					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV16-180822/2236
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV16-180822/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv260p_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.05					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV26-180822/2238
Improper Neutralization of Special Elements used in an OS Command ('OS	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV26-180822/2239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**		
Product: rv260w_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.05					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV26-180822/2240
Improper Neutralization of Special Elements used in an	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-	O-CIS-RV26-180822/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	vuln-CbVp4SUR	
Product: rv260_firmware					
Affected Version(s): * Up to (excluding) 1.0.01.05					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV26-180822/2242
Improper Neutralizat	10-Aug-2022	10	Multiple vulnerabilities in	https://tools.cisco.com/securi	O-CIS-RV26-180822/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	
Product: rv340w_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.26					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20841		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2245
Affected Version(s): * Up to (excluding) 1.0.03.28					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2022-20842**		
Product: rv340_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.26					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2247
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**		
Affected Version(s): * Up to (excluding) 1.0.03.28					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20842**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2249
Product: rv345p_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.26					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-Aug-2022	10	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2251
Affected Version(s): * Up to (excluding) 1.0.03.28					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-	O-CIS-RV34-180822/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20842**	vuln-CbVp4SUR	
Product: rv345_firmware					
Affected Version(s): * Up to (excluding) 1.0.03.26					
Improper Input Validation	10-Aug-2022	9	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20841**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2253
Improper Neutralizat	10-Aug-2022	10	Multiple vulnerabilities in	https://tools.cisco.com/securi	O-CIS-RV34-180822/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2022-20827**	ty/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	
Affected Version(s): * Up to (excluding) 1.0.03.28					
Improper Input Validation	10-Aug-2022	9.8	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR	O-CIS-RV34-180822/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20842		
Vendor: contiki-ng					
Product: contiki-ng					
Affected Version(s): * Up to (excluding) 4.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Aug-2022	9.8	Contiki-NG is an open-source, cross-platform operating system for IoT devices. In the RPL-Classic routing protocol implementation in the Contiki-NG operating system, an incoming DODAG Information Option (DIO) control message can contain a prefix information option with a length parameter. The value of the length parameter is not validated, however, and it is possible to cause a buffer overflow when copying the prefix in the set_ip_from_prefix function. This vulnerability affects anyone running a Contiki-NG version prior to 4.7 that can receive RPL DIO messages from external parties. To obtain a patched version, users should upgrade to Contiki-NG 4.7 or later.	https://github.com/contiki-ng/contiki-ng/pull/1589/commits/4fffab0e632c4d01910fa957d1fd9ef321eb87d2, https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-9rm9-3phh-p4wm	O-CON-CONT-180822/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			There are no workarounds for this issue. **CVE ID : CVE-2022-35927**		
Affected Version(s): * Up to (excluding) 4.8					
Out-of-bounds Read	04-Aug-2022	7.5	Contiki-NG is an open-source, cross-platform operating system for IoT devices. Because of insufficient validation of IPv6 neighbor discovery options in Contiki-NG, attackers can send neighbor solicitation packets that trigger an out-of-bounds read. The problem exists in the module os/net/ipv6/uip-nd6.c, where memory read operations from the main packet buffer, <code>uip_buf</code>, are not checked if they go out of bounds. In particular, this problem can occur when attempting to read the 2-byte option header and the Source Link-Layer Address Option (SLLAO). This attack requires ipv6 be enabled for the network. The problem has been	https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-4hpq-4f53-w386, https://github.com/contiki-ng/contiki-ng/pull/1654/commits/a4597001d50a04f4b9c78f323ba731e2f979802c, https://github.com/contiki-ng/contiki-ng/pull/1654	O-CON-CONT-180822/2257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patched in the develop branch of Contiki-NG. The upcoming 4.8 release of Contiki-NG will include the patch.Users unable to upgrade may apply the patch in Contiki-NG PR #1654. **CVE ID : CVE-2022-35926**		
Vendor: Dd-wrt					
Product: dd-wrt					
Affected Version(s): From (including) 32270 Up to (including) 48599					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of DD-WRT Revision 32270 - Revision 48599. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability. **CVE ID : CVE-2022-27631**	N/A	O-DD--DD-W-180822/2258
Vendor: Dlink					
Product: dir-818l_firmware					
Affected Version(s): 105b01					
N/A	03-Aug-2022	9.8	D-LINK DIR-818LW A1:DIR818L_FW105 b01 was discovered to contain a remote	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--180822/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution (RCE) vulnerability via the function ssdpcgi_main. **CVE ID : CVE-2022-35619**		
N/A	03-Aug-2022	9.8	D-LINK DIR-818LW A1:DIR818L_FW105 b01 was discovered to contain a remote code execution (RCE) vulnerability via the function binary.soapcgi_main. **CVE ID : CVE-2022-35620**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--180822/2260
Product: dir820la1_firmware					
Affected Version(s): 102b22					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-Aug-2022	9.8	D-Link DIR810LA1_FW102B22 was discovered to contain a command injection vulnerability via the Ping_addr function. **CVE ID : CVE-2022-34974**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR8-180822/2261
Affected Version(s): 106b02					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Aug-2022	7.5	D-Link DIR820LA1_FW106B02 was discovered to contain a buffer overflow via the nextPage parameter at ping.ccp. **CVE ID : CVE-2022-34973**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR8-180822/2262
Vendor: Fedoraproject					
Product: fedora					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 35					
Use After Free	05-Aug-2022	7.1	A use-after-free flaw was found in the Linux kernel in log_replay in fs/ntfs3/fslog.c in the NTFS journal. This flaw allows a local attacker to crash the system and leads to a kernel information leak problem. **CVE ID : CVE-2022-1973**	N/A	O-FED-FEDO-180822/2263
Affected Version(s): 36					
Use After Free	05-Aug-2022	7.8	A flaw was found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the offset to get the page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition. **CVE ID : CVE-2022-1158**	N/A	O-FED-FEDO-180822/2264
N/A	10-Aug-2022	7.5	A too-short encoded message can cause a panic in Float.GobDecode and Rat GobDecode in	https://pkg.go.dev/vuln/GO-2022-0537, https://go.dev/cl/417774,	O-FED-FEDO-180822/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			math/big in Go before 1.17.13 and 1.18.5, potentially allowing a denial of service. **CVE ID : CVE-2022-32189**	https://go.googlesource.com/go/+/055113ef364337607e3e72ed7d48df67fde6fc66	
Use After Free	05-Aug-2022	7.1	A use-after-free flaw was found in the Linux kernel in log_replay in fs/ntfs3/fslog.c in the NTFS journal. This flaw allows a local attacker to crash the system and leads to a kernel information leak problem. **CVE ID : CVE-2022-1973**	N/A	O-FED-FEDO-180822/2266
Vendor: Fortinet					
Product: fortios					
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.14					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 5.2.0 Up to (including) 5.2.15					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 5.4.0 Up to (including) 5.4.13					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 5.6.0 Up to (including) 5.6.14					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.14					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.10					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7,	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 6.2.0 Up to (including) 6.2.11					
Incorrect Authorization	03-Aug-2022	4.3	An improper access control vulnerability [CWE-284] in FortiOS versions 6.2.0 through 6.2.11, 6.4.0 through 6.4.8 and 7.0.0 through 7.0.5 may allow an authenticated attacker with a restricted user profile to gather the checksum information about the other VDOMs via CLI commands.	https://fortiguard.com/psirt/FG-IR-22-036	O-FOR-FORT-180822/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23442		
Affected Version(s): From (including) 6.4.0 Up to (excluding) 6.4.8					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1, FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments.	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22299		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.8					
Incorrect Authorization	03-Aug-2022	4.3	An improper access control vulnerability [CWE-284] in FortiOS versions 6.2.0 through 6.2.11, 6.4.0 through 6.4.8 and 7.0.0 through 7.0.5 may allow an authenticated attacker with a restricted user profile to gather the checksum information about the other VDOMs via CLI commands. **CVE ID : CVE-2022-23442**	https://fortiguard.com/psirt/FG-IR-22-036	O-FOR-FORT-180822/2275
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.2					
Use of Externally-Controlled Format String	05-Aug-2022	7.8	A format string vulnerability [CWE-134] in the command line interpreter of FortiADC version 6.0.0 through 6.0.4, FortiADC version 6.1.0 through 6.1.5, FortiADC version 6.2.0 through 6.2.1, FortiProxy version 1.0.0 through 1.0.7, FortiProxy version 1.1.0 through 1.1.6, FortiProxy version 1.2.0 through 1.2.13, FortiProxy version 2.0.0 through 2.0.7, FortiProxy version 7.0.0 through 7.0.1,	https://fortiguard.com/psirt/FG-IR-21-235	O-FOR-FORT-180822/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.2, FortiMail version 6.4.0 through 6.4.5, FortiMail version 7.0.0 through 7.0.2 may allow an authenticated user to execute unauthorized code or commands via specially crafted command arguments. **CVE ID : CVE-2022-22299**		
Affected Version(s): From (including) 7.0.0 Up to (including) 7.0.5					
Incorrect Authorization	03-Aug-2022	4.3	An improper access control vulnerability [CWE-284] in FortiOS versions 6.2.0 through 6.2.11, 6.4.0 through 6.4.8 and 7.0.0 through 7.0.5 may allow an authenticated attacker with a restricted user profile to gather the checksum information about the other VDOMs via CLI commands. **CVE ID : CVE-2022-23442**	https://fortiguard.com/psirt/FG-IR-22-036	O-FOR-FORT-180822/2277
Vendor: freshtomato					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: freshtomato					
Affected Version(s): 2022.1					
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of FreshTomato 2022.1. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.The `freshtomato-mips` has a vulnerable URL-decoding feature that can lead to memory corruption. **CVE ID : CVE-2022-28664**	N/A	O-FRE-FRES-180822/2278
Out-of-bounds Write	05-Aug-2022	9.8	A memory corruption vulnerability exists in the httpd unescape functionality of FreshTomato 2022.1. A specially-crafted HTTP request can lead to memory corruption. An attacker can send a network request to trigger this vulnerability.The `freshtomato-arm` has a vulnerable URL-decoding	N/A	O-FRE-FRES-180822/2279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			feature that can lead to memory corruption. **CVE ID : CVE-2022-28665**		
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	11-Aug-2022	9.8	In BuildDevIDResponse of miscdatabuilder.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-229621649References: N/A **CVE ID : CVE-2022-20237**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2280
Externally Controlled Reference to a Resource in Another Sphere	10-Aug-2022	9.8	'remap_pfn_range' here may map out of size kernel memory (for example, may map the kernel area), and because the 'vma->vm_page_prot' can also be controlled by userspace, so userspace may map	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the kernel area to be writable, which is easy to be exploitedProduct: AndroidVersions: Android SoCAndroid ID: A-233972091 **CVE ID : CVE-2022-20239**		
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-188935887References: N/A **CVE ID : CVE-2022-20381**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2282
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-229632566References: N/A **CVE ID : CVE-2022-20365**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2283
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-234657153References: N/A **CVE ID : CVE-2022-20378**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2284
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-224546354References: Upstream kernel **CVE ID : CVE-2022-20368**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-211727306References: N/A **CVE ID : CVE-2022-20384**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2286
Out-of-bounds Write	11-Aug-2022	9.8	In cd_CodeMsg of cd_codec.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-225178325References: N/A **CVE ID : CVE-2022-20400**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2287
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-218701042References: N/A **CVE ID : CVE-2022-20402**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2288
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-207975764References: N/A	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20403		
N/A	11-Aug-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-216363416References: N/A **CVE ID : CVE-2022-20405**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2290
Use After Free	12-Aug-2022	8.8	Use after free in Offline in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2623**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1337798	O-GOO-ANDR-180822/2291
Improper Privilege Management	12-Aug-2022	8.8	In Wi-Fi, there is a permissions bypass. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-223377547 **CVE ID : CVE-2022-20254**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	11-Aug-2022	7.8	In several functions of mali_gralloc_reference.cpp, there is a possible arbitrary code execution due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-212804042References: N/A **CVE ID : CVE-2022-20180**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2293
Inadequate Encryption Strength	11-Aug-2022	7.8	On specific devices, there is a possible bypass of configuration integrity due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-201078231References: N/A	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20374		
Integer Overflow or Wraparound	11-Aug-2022	7.8	In AllocateInternalBuffers of g3aa_buffer_allocator.cc, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222408847References: N/A **CVE ID : CVE-2022-20383**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2295
Out-of-bounds Read	11-Aug-2022	7.5	In LteRrcNrProAsnDecode of LteRrcNr_Codec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernelAndroid ID: A-180956894References: N/A **CVE ID : CVE-2022-20375**		
N/A	11-Aug-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-215730643References: N/A **CVE ID : CVE-2022-20370**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2297
N/A	11-Aug-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-212625740References: N/A **CVE ID : CVE-2022-20380**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2298
Out-of-bounds Read	11-Aug-2022	7.5	In SAEMM_RetrievEPLMNList of SAEMM_ContextManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure post-authentication with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernelAndroid ID: A-226446030References: N/A **CVE ID : CVE-2022-20401**		
N/A	11-Aug-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-205714161References: N/A **CVE ID : CVE-2022-20404**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2300
N/A	11-Aug-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-184676385References: N/A **CVE ID : CVE-2022-20406**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2301
N/A	11-Aug-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-210916981References: N/A **CVE ID : CVE-2022-20407**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2302
N/A	11-Aug-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-204782372References: N/A **CVE ID : CVE-2022-20408**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2303
Use After Free	11-Aug-2022	6.7	In exynos5_i2c_irq of (TBD), there is a possible out of bounds write due to	https://source.android.com/security/bulleti	O-GOO-ANDR-180822/2304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-195480799References: N/A **CVE ID : CVE-2022-20372**	n/pixel/2022-08-01	
Use After Free	11-Aug-2022	6.7	In trusty_log_seq_start of trusty-log.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-216130110References: N/A **CVE ID : CVE-2022-20376**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2305
Use After Free	11-Aug-2022	6.7	In bdi_put and bdi_unregister of backing-dev.c, there is a possible memory corruption due to a use after free. This	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2306

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.Product: AndroidVersions: Android kernelAndroid ID: A-182815710References: Upstream kernel **CVE ID : CVE-2022-20158**		
Use After Free	11-Aug-2022	6.7	In lwis_buffer_alloc of lwis_buffer.c, there is a possible arbitrary code execution 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.Product: AndroidVersions: Android kernelAndroid ID: A-209436980References: N/A **CVE ID : CVE-2022-20379**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2307
Out-of-bounds Write	11-Aug-2022	6.7	In (TBD) of (TBD), there is a possible out of bounds write due to kernel stack overflow. This could lead to local escalation of	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-214245176References: Upstream kernel **CVE ID : CVE-2022-20382**		
Integer Overflow or Wraparound	11-Aug-2022	6.7	In ioctl_dpm_clk_update of lwis_ioctl.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-225877745References: N/A **CVE ID : CVE-2022-20366**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2309
Integer Overflow or Wraparound	11-Aug-2022	6.7	In construct_transaction of lwis_ioctl.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-225877459References: N/A **CVE ID : CVE-2022-20367**		
Out-of-bounds Write	11-Aug-2022	6.7	In v4l2_m2m_querybuf of v4l2-mem2mem.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-223375145References: Upstream kernel **CVE ID : CVE-2022-20369**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2311
N/A	11-Aug-2022	6.7	In TBD of keymaster_ipc.cpp, there is a possible to force gatekeeper, fingerprint, and faceauth to use a known HMAC key.	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222339795References: N/A **CVE ID : CVE-2022-20377**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-Aug-2022	6.4	In dm_bow_dtr and related functions of dm-bow.c, 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.Product: AndroidVersions: Android kernelAndroid ID: A-195565510References: Upstream kernel **CVE ID : CVE-2022-20371**	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2313
Concurrent Execution using Shared Resource with Improper	11-Aug-2022	6.4	In st21nfc_loc_set_polaritymode of fc/st21nfc.c, there is a possible use after free due to a race condition. This could	https://source.android.com/security/bulletin/pixel/2022-08-01	O-GOO-ANDR-180822/2314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-208269510References: N/A **CVE ID : CVE-2022-20373**		
N/A	12-Aug-2022	5.7	In Bluetooth, there is a possible cleanup failure due to an uncaught exception. This could lead to remote denial of service in Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-224545125 **CVE ID : CVE-2022-20253**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2315
N/A	12-Aug-2022	4.3	Inappropriate implementation in Fullscreen API in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar)	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1320538	O-GOO-ANDR-180822/2316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. **CVE ID : CVE-2022-2611**		
Affected Version(s): 10.0					
N/A	10-Aug-2022	9.8	In btif_dm_auth_cmpl_evt of btif_dm.cc, there is a possible vulnerability in Cross-Transport Key Derivation due to Weakness in Bluetooth Standard. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-231161832 **CVE ID : CVE-2022-20361**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2317
Integer Overflow or Wraparound	05-Aug-2022	9.8	Improper input validation in baseband prior to SMR Aug-2022 Release 1 allows attackers to cause integer overflow to heap overflow. **CVE ID : CVE-2022-33719**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2318
N/A	10-Aug-2022	8.8	In onAttach of ConnectedDeviceDashboardFragment.jav	https://source.android.com/s	O-GOO-ANDR-180822/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228450811 **CVE ID : CVE-2022-20347**	ecurity/bulletin/2022-08-01	
Incorrect Default Permissions	10-Aug-2022	7.8	In updateState of LocationServicesWifiScanningPreferenceController.java, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315529	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20348		
Incorrect Default Permissions	10-Aug-2022	7.8	In WifiScanningPreferenceController and BluetoothScanningPreferenceController, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315522 **CVE ID : CVE-2022-20349**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2321
Incorrect Default Permissions	10-Aug-2022	7.8	In setChecked of SecureNfcPreferenceController.java, there is a missing permission check. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			11 Android-12 Android-12LAndroid ID: A-228314987 **CVE ID : CVE-2022-20360**		
Improper Privilege Management	05-Aug-2022	7.8	Improper Privilege Management vulnerability in Game Optimizing Service prior to versions 3.3.04.0 in Android 10, and 3.5.04.8 in Android 11 and above allows local attacker to execute hidden function for developer by changing package name. **CVE ID : CVE-2022-36833**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	O-GOO-ANDR-180822/2323
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	10-Aug-2022	7	In stealReceiveChannel of EventThread.cpp, there is a possible way to interfere with process communication due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12LAndroid ID: A-232541124 **CVE ID : CVE-2022-20344**		
Out-of-bounds Read	10-Aug-2022	6.5	In updateAudioTrackInfoFromESDS_MPEG4Audio of MPEG4Extractor.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-230493653 **CVE ID : CVE-2022-20346**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2325
Improper Restriction of Rendered UI Layers or Frames	05-Aug-2022	6.1	A vulnerable code in onCreate of BluetoothScanDialog prior to SMR Aug-2022 Release 1, allows attackers to trick the user to select an unwanted bluetooth device via tapjacking/overlay attack. **CVE ID : CVE-2022-33723**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	05-Aug-2022	6.1	A vulnerable code in onCreate of SecDevicePickerDialog prior to SMR Aug-2022 Release 1, allows attackers to trick the user to select an unwanted bluetooth device via tapjacking/overlay attack. **CVE ID : CVE-2022-33727**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2327
Improper Input Validation	10-Aug-2022	5.5	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible way to trick the victim to grant notification access to the wrong app due to improper input validation. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228178437 **CVE ID : CVE-2022-20350**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2328
Improper Input Validation	10-Aug-2022	5.5	In onSaveRingtone of DefaultRingtonePreference.java, there is a possible inappropriate file	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221041256 **CVE ID : CVE-2022-20353**		
Improper Input Validation	10-Aug-2022	5.5	In get of PacProxyService.java , there is a possible system service crash due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-219498290 **CVE ID : CVE-2022-20355**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2330
Incorrect Default Permissions	10-Aug-2022	3.3	In startSync of AbstractThreadedSyncAdapter.java, there is a possible way to access protected content of content	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			providers due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-203229608 **CVE ID : CVE-2022-20358**		
N/A	05-Aug-2022	3.3	Improper access control vulnerability in SemWifiApBroadcastReceiver prior to SMR Aug-2022 Release 1 allows attacker to reset a setting value related to mobile hotspot. **CVE ID : CVE-2022-33714**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2332
N/A	05-Aug-2022	3.3	An improper access control vulnerability in Wi-Fi Service prior to SMR AUG-2022 Release 1 allows untrusted applications to manipulate the list of apps that can use mobile data. **CVE ID : CVE-2022-33718**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	05-Aug-2022	3.3	Exposure of Sensitive Information in Samsung Dialer application?prior to SMR Aug-2022 Release 1 allows local attackers to access ICCID via log. **CVE ID : CVE-2022-33724**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2334
N/A	05-Aug-2022	3.3	A vulnerability using PendingIntent in Knox VPN prior to SMR Aug-2022 Release 1 allows attackers to access content providers with system privilege. **CVE ID : CVE-2022-33725**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2335
N/A	05-Aug-2022	3.3	Unprotected dynamic receiver in Samsung Galaxy Friends prior to SMR Aug-2022 Release 1 allows attacker to launch activity. **CVE ID : CVE-2022-33726**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2336
N/A	05-Aug-2022	3.3	Exposure of sensitive information in Bluetooth prior to SMR Aug-2022 Release 1 allows local attackers to access connected BT macAddress via Settings.Gloabal.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33728		
N/A	05-Aug-2022	3.3	Improper restriction of broadcasting Intent in ConfirmConnectActivity of?NFC prior to SMR Aug-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-33729**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2338
N/A	05-Aug-2022	2.4	Improper authentication vulnerability in AppLock prior to SMR Aug-2022 Release 1 allows physical attacker to access Chrome locked by AppLock via new tap shortcut. **CVE ID : CVE-2022-33720**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2339
Affected Version(s): 11.0					
N/A	10-Aug-2022	9.8	In btif_dm_auth_cmpl_evt of btif_dm.cc, there is a possible vulnerability in Cross-Transport Key Derivation due to Weakness in Bluetooth Standard. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-231161832 **CVE ID : CVE-2022-20361**		
Integer Overflow or Wraparound	05-Aug-2022	9.8	Improper input validation in baseband prior to SMR Aug-2022 Release 1 allows attackers to cause integer overflow to heap overflow. **CVE ID : CVE-2022-33719**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2341
N/A	10-Aug-2022	8.8	In onAttach of ConnectedDeviceDashboardFragment.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228450811	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20347		
Incorrect Default Permissions	10-Aug-2022	7.8	In updateState of LocationServicesWifiScanningPreferenceController.java, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315529 **CVE ID : CVE-2022-20348**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2343
Incorrect Default Permissions	10-Aug-2022	7.8	In WifiScanningPreferenceController and BluetoothScanningPreferenceController, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315522 **CVE ID : CVE-2022-20349**		
Improper Privilege Management	05-Aug-2022	7.8	Improper Privilege Management vulnerability in Game Optimizing Service prior to versions 3.3.04.0 in Android 10, and 3.5.04.8 in Android 11 and above allows local attacker to execute hidden function for developer by changing package name. **CVE ID : CVE-2022-36833**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	O-GOO-ANDR-180822/2345
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415; Issue ID: ALPS07025415.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26429		
N/A	10-Aug-2022	7.8	In onDefaultNetworkChanged of Vpn.java, there is a possible way to disable VPN due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-219546241 **CVE ID : CVE-2022-20354**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2347
Improper Input Validation	10-Aug-2022	7.8	In shouldAllowFgsWhileInUsePermissionLocked of ActiveServices.java, there is a possible way to start foreground service from background due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-215003903 **CVE ID : CVE-2022-20356**		
Incorrect Default Permissions	10-Aug-2022	7.8	In setChecked of SecureNfcPreferenceController.java, there is a missing permission check. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228314987 **CVE ID : CVE-2022-20360**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2349
N/A	05-Aug-2022	7.1	Improper access control vulnerability in DesktopSystemUI prior to SMR Aug-2022 Release 1 allows attackers to enable and disable arbitrary components. **CVE ID : CVE-2022-33731**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2350
Concurrent Execution using	10-Aug-2022	7	In stealReceiveChannel of EventThread.cpp,	https://source.android.com/s	O-GOO-ANDR-180822/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			there is a possible way to interfere with process communication due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-232541124 **CVE ID : CVE-2022-20344**	ecurity/bulletin/2022-08-01	
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2352
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, 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/August-2022	O-GOO-ANDR-180822/2353

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: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2354
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2356
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2357
Out-of-bounds Write	01-Aug-2022	6.7	In camera isp, there is a possible out of bounds write due to	https://corp.mediatek.com/product-security-	O-GOO-ANDR-180822/2358

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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2359
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation. Patch ID: ALPS07085540; Issue ID: ALPS07085540. **CVE ID : CVE-2022-26427**		
Out-of-bounds Read	10-Aug-2022	6.5	In updateAudioTrackInfoFromESDS_MPEG4Audio of MPEG4Extractor.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-230493653 **CVE ID : CVE-2022-20346**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2361
Concurrent Execution using Shared Resource with Improper Synchronization	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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/August-2022	O-GOO-ANDR-180822/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			exploitation. Patch ID: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2363
Improper Restriction of Rendered UI Layers or Frames	05-Aug-2022	6.1	A vulnerable code in onCreate of BluetoothScanDialog prior to SMR Aug-2022 Release 1, allows attackers to trick the user to select an unwanted bluetooth device via tapjacking/overlay attack. **CVE ID : CVE-2022-33723**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2364
Improper Restriction of Rendered UI Layers or Frames	05-Aug-2022	6.1	A vulnerable code in onCreate of SecDevicePickerDialog prior to SMR Aug-2022 Release 1, allows attackers to	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trick the user to select an unwanted bluetooth device via tapjacking/overlay attack. **CVE ID : CVE-2022-33727**		
Improper Input Validation	10-Aug-2022	5.5	In onSaveRingtone of DefaultRingtonePreference.java, there is a possible inappropriate file read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221041256 **CVE ID : CVE-2022-20353**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2366
Improper Input Validation	10-Aug-2022	5.5	In get of PacProxyService.java, there is a possible system service crash due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12LAndroid ID: A-219498290 **CVE ID : CVE-2022-20355**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	5.5	Improper access control and path traversal vulnerability in LauncherProvider prior to SMR Aug-2022 Release 1 allow local attacker to access files of One UI. **CVE ID : CVE-2022-33715**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2368
Improper Input Validation	10-Aug-2022	5.5	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible way to trick the victim to grant notification access to the wrong app due to improper input validation. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228178437 **CVE ID : CVE-2022-20350**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06479306; Issue ID: ALPS06479306. **CVE ID : CVE-2022-21790**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2370
Use of Uninitialized Resource	05-Aug-2022	4.4	An absence of variable initialization in ICCC TA prior to SMR Aug-2022 Release 1 allows local attacker to read uninitialized memory. **CVE ID : CVE-2022-33716**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2371
Out-of-bounds Read	05-Aug-2022	4.4	A missing input validation before memory read in SEM TA prior to SMR Aug-2022 Release 1 allows local attackers to read out of bound memory. **CVE ID : CVE-2022-33717**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2372
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, there is a possible out of bounds read due to a missing bounds	https://corp.mediatek.com/product-security-	O-GOO-ANDR-180822/2373

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: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**	bulletin/August-2022	
Incorrect Default Permissions	10-Aug-2022	3.3	In startSync of AbstractThreadedSyncAdapter.java, there is a possible way to access protected content of content providers due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-203229608 **CVE ID : CVE-2022-20358**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2374
N/A	05-Aug-2022	3.3	Improper access control vulnerability in SemWifiApBroadcastReceiver prior to	https://security.samsungmobile.com/securityUpdate.smsb?y	O-GOO-ANDR-180822/2375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMR Aug-2022 Release 1 allows attacker to reset a setting value related to mobile hotspot. **CVE ID : CVE-2022-33714**	ear=2022&month=08	
N/A	05-Aug-2022	3.3	An improper access control vulnerability in Wi-Fi Service prior to SMR AUG-2022 Release 1 allows untrusted applications to manipulate the list of apps that can use mobile data. **CVE ID : CVE-2022-33718**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2376
Cleartext Transmission of Sensitive Information	05-Aug-2022	3.3	Exposure of Sensitive Information in Samsung Dialer application?prior to SMR Aug-2022 Release 1 allows local attackers to access ICCID via log. **CVE ID : CVE-2022-33724**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2377
N/A	05-Aug-2022	3.3	A vulnerability using PendingIntent in Knox VPN prior to SMR Aug-2022 Release 1 allows attackers to access content providers with system privilege. **CVE ID : CVE-2022-33725**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	05-Aug-2022	3.3	Exposure of sensitive information in Bluetooth prior to SMR Aug-2022 Release 1 allows local attackers to access connected BT macAddress via Settings.Gloabal. **CVE ID : CVE-2022-33728**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2379
N/A	05-Aug-2022	3.3	Improper restriction of broadcasting Intent in ConfirmConnectActivity of?NFC prior to SMR Aug-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-33729**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2380
N/A	05-Aug-2022	3.3	Unprotected dynamic receiver in Samsung Galaxy Friends prior to SMR Aug-2022 Release 1 allows attacker to launch activity. **CVE ID : CVE-2022-33726**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2381
N/A	05-Aug-2022	2.4	Improper authentication vulnerability in AppLock prior to SMR Aug-2022 Release 1 allows physical attacker to access Chrome locked by AppLock via new tap shortcut.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33720		
Affected Version(s): 12.0					
N/A	10-Aug-2022	9.8	In btif_dm_auth_cmpl_evt of btif_dm.cc, there is a possible vulnerability in Cross-Transport Key Derivation due to Weakness in Bluetooth Standard. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-231161832 **CVE ID : CVE-2022-20361**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2383
Integer Overflow or Wraparound	05-Aug-2022	9.8	Improper input validation in baseband prior to SMR Aug-2022 Release 1 allows attackers to cause integer overflow to heap overflow. **CVE ID : CVE-2022-33719**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2384
Out-of-bounds Write	10-Aug-2022	8.8	In l2cble_process_sig_cmd of l2c_ble.cc, there is a possible out of bounds write	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-230494481 **CVE ID : CVE-2022-20345**		
N/A	10-Aug-2022	8.8	In onAttach of ConnectedDeviceDashboardFragment.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228450811 **CVE ID : CVE-2022-20347**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2386
Incorrect Default	10-Aug-2022	7.8	In updateState of LocationServicesWifiScanningPreferenceC	https://source.android.com/s	O-GOO-ANDR-180822/2387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			ontroller.java, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315529 **CVE ID : CVE-2022-20348**	ecurity/bulletin/2022-08-01	
Incorrect Default Permissions	10-Aug-2022	7.8	In WifiScanningPreferenceController and BluetoothScanningPreferenceController, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315522	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20349		
N/A	10-Aug-2022	7.8	In onDefaultNetworkChanged of Vpn.java, there is a possible way to disable VPN due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-219546241 **CVE ID : CVE-2022-20354**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2389
Improper Input Validation	10-Aug-2022	7.8	In shouldAllowFgsWhileInUsePermissionLocked of ActiveServices.java, there is a possible way to start foreground service from background due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-215003903 **CVE ID : CVE-2022-20356**		
Incorrect Default Permissions	10-Aug-2022	7.8	In setChecked of SecureNfcPreferenceController.java, there is a missing permission check. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228314987 **CVE ID : CVE-2022-20360**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2391
Incorrect Default Permissions	01-Aug-2022	7.8	In cta, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07025415;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07025415. **CVE ID : CVE-2022-26429**		
N/A	05-Aug-2022	7.1	Improper access control vulnerability in Samsung Dex for PC prior to SMR Aug-2022 Release 1 allows local attackers to scan and connect to PC by unprotected binder call. **CVE ID : CVE-2022-33732**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2393
N/A	05-Aug-2022	7.1	Improper access control vulnerability in DesktopSystemUI prior to SMR Aug-2022 Release 1 allows attackers to enable and disable arbitrary components. **CVE ID : CVE-2022-33731**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2394
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	10-Aug-2022	7	In stealReceiveChannel of EventThread.cpp, there is a possible way to interfere with process communication due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-232541124 **CVE ID : CVE-2022-20344**		
Out-of-bounds Write	05-Aug-2022	6.8	Heap-based buffer overflow vulnerability in Samsung Dex for PC prior to SMR Aug-2022 Release 1 allows arbitrary code execution by physical attackers. **CVE ID : CVE-2022-33730**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2396
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2397
Out-of-bounds Write	01-Aug-2022	6.7	In camera isp, 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/August-2022	O-GOO-ANDR-180822/2398

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: ALPS07085410; Issue ID: ALPS07085410. **CVE ID : CVE-2022-21792**		
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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: ALPS07085486; Issue ID: ALPS07085486. **CVE ID : CVE-2022-26426**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2399
Out-of-bounds Write	01-Aug-2022	6.7	In camera 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	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: ALPS07085540; Issue ID: ALPS07085540. **CVE ID : CVE-2022-26427**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2401
N/A	01-Aug-2022	6.7	In scp, there is a possible undefined behavior due to incorrect error handling. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06988728; Issue ID: ALPS06988728. **CVE ID : CVE-2022-21788**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2403
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2404
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2406
Out-of-bounds Read	10-Aug-2022	6.5	In updateAudioTrackInfoFromESDS_MPEG4Audio of MPEG4Extractor.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-230493653 **CVE ID : CVE-2022-20346**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In video codec, there is a possible memory corruption 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: ALPS06521260; Issue ID: ALPS06521260. **CVE ID : CVE-2022-26428**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2408
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-Aug-2022	6.4	In audio ipi, there is a possible memory corruption 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: ALPS06478101; Issue ID: ALPS06478101. **CVE ID : CVE-2022-21789**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	05-Aug-2022	6.1	A vulnerable code in onCreate of BluetoothScanDialog prior to SMR Aug-2022 Release 1, allows attackers to trick the user to select an unwanted bluetooth device via tapjacking/overlay attack. **CVE ID : CVE-2022-33723**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2410
Improper Restriction of Rendered UI Layers or Frames	05-Aug-2022	6.1	A vulnerable code in onCreate of SecDevicePickerDialog prior to SMR Aug-2022 Release 1, allows attackers to trick the user to select an unwanted bluetooth device via tapjacking/overlay attack. **CVE ID : CVE-2022-33727**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2411
Missing Initialization of Resource	10-Aug-2022	5.5	In writeToParcel of SurfaceControl.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12LAndroid ID: A-214999987 **CVE ID : CVE-2022-20357**		
Improper Input Validation	10-Aug-2022	5.5	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible way to trick the victim to grant notification access to the wrong app due to improper input validation. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228178437 **CVE ID : CVE-2022-20350**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2413
N/A	05-Aug-2022	5.5	A vulnerability using PendingIntent in DeX for PC prior to SMR Aug-2022 Release 1 allows attackers to access files with system privilege. **CVE ID : CVE-2022-33721**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2414
Incorrect Default Permissions	10-Aug-2022	5.5	In addProviderRequestListener of LocationManagerSer	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vice.java, there is a possible way to learn which packages request location information due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-222473855 **CVE ID : CVE-2022-20352**		
Improper Input Validation	10-Aug-2022	5.5	In onSaveRingtone of DefaultRingtonePreference.java, there is a possible inappropriate file read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-221041256 **CVE ID : CVE-2022-20353**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	10-Aug-2022	5.5	In get of PacProxyService.java , there is a possible system service crash due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-219498290 **CVE ID : CVE-2022-20355**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2417
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	5.5	Improper access control and path traversal vulnerability in LauncherProvider prior to SMR Aug-2022 Release 1 allow local attacker to access files of One UI. **CVE ID : CVE-2022-33715**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2418
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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/August-2022	O-GOO-ANDR-180822/2419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS06478059; Issue ID: ALPS06478059. **CVE ID : CVE-2022-21791**		
Out-of-bounds Read	01-Aug-2022	4.4	In camera isp, 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: ALPS06479306; Issue ID: ALPS06479306. **CVE ID : CVE-2022-21790**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2420
Out-of-bounds Read	01-Aug-2022	4.4	In emi mpu, 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: ALPS07023666; Issue ID: ALPS07023666. **CVE ID : CVE-2022-26436**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-GOO-ANDR-180822/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Uninitialized Resource	05-Aug-2022	4.4	An absence of variable initialization in ICCC TA prior to SMR Aug-2022 Release 1 allows local attacker to read uninitialized memory. **CVE ID : CVE-2022-33716**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2422
Out-of-bounds Read	05-Aug-2022	4.4	A missing input validation before memory read in SEM TA prior to SMR Aug-2022 Release 1 allows local attackers to read out of bound memory. **CVE ID : CVE-2022-33717**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2423
N/A	05-Aug-2022	3.3	Implicit Intent hijacking vulnerability in Smart View prior to SMR Aug-2022 Release 1 allows attacker to access connected device MAC address. **CVE ID : CVE-2022-33722**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2424
N/A	05-Aug-2022	3.3	Improper access control vulnerability in SemWifiApBroadcastReceiver prior to SMR Aug-2022 Release 1 allows attacker to reset a setting value related to mobile hotspot.	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33714		
Cleartext Transmission of Sensitive Information	05-Aug-2022	3.3	Exposure of Sensitive Information in Samsung Dialer application?prior to SMR Aug-2022 Release 1 allows local attackers to access ICCID via log. **CVE ID : CVE-2022-33724**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2426
N/A	05-Aug-2022	3.3	An improper access control vulnerability in Wi-Fi Service prior to SMR AUG-2022 Release 1 allows untrusted applications to manipulate the list of apps that can use mobile data. **CVE ID : CVE-2022-33718**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2427
Incorrect Default Permissions	10-Aug-2022	3.3	In startSync of AbstractThreadedSyncAdapter.java, there is a possible way to access protected content of content providers due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-203229608 **CVE ID : CVE-2022-20358**		
N/A	05-Aug-2022	3.3	Exposure of sensitive information in Bluetooth prior to SMR Aug-2022 Release 1 allows local attackers to access connected BT macAddress via Settings.Gloabal. **CVE ID : CVE-2022-33728**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2429
N/A	05-Aug-2022	3.3	Improper restriction of broadcasting Intent in ConfirmConnectActivity of?NFC prior to SMR Aug-2022 Release 1 leaks MAC address of the connected Bluetooth device. **CVE ID : CVE-2022-33729**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2430
N/A	05-Aug-2022	3.3	Unprotected dynamic receiver in Samsung Galaxy Friends prior to SMR Aug-2022 Release 1 allows attacker to launch activity. **CVE ID : CVE-2022-33726**	https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=08	O-GOO-ANDR-180822/2431
Affected Version(s): 12.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	10-Aug-2022	9.8	In btif_dm_auth_cmpl_evt of btif_dm.cc, there is a possible vulnerability in Cross-Transport Key Derivation due to Weakness in Bluetooth Standard. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-231161832 **CVE ID : CVE-2022-20361**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2432
Out-of-bounds Write	10-Aug-2022	8.8	In l2cble_process_sig_cmd of l2c_ble.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-230494481	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20345		
N/A	10-Aug-2022	8.8	In onAttach of ConnectedDeviceDashboardFragment.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228450811 **CVE ID : CVE-2022-20347**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2434
Incorrect Default Permissions	10-Aug-2022	7.8	In updateState of LocationServicesWifiScanningPreferenceController.java, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315529 **CVE ID : CVE-2022-20348**		
Incorrect Default Permissions	10-Aug-2022	7.8	In WifiScanningPreferenceController and BluetoothScanningPreferenceController, there is a possible admin restriction bypass due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315522 **CVE ID : CVE-2022-20349**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2436
N/A	10-Aug-2022	7.8	In onDefaultNetworkChanged of Vpn.java, there is a possible way to disable VPN due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed.	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-219546241 **CVE ID : CVE-2022-20354**		
Improper Input Validation	10-Aug-2022	7.8	In shouldAllowFgsWhileInUsePermissionLocked of ActiveServices.java, there is a possible way to start foreground service from background due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-215003903 **CVE ID : CVE-2022-20356**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2438
Incorrect Default Permissions	10-Aug-2022	7.8	In setChecked of SecureNfcPreferenceController.java, there is a missing permission check. This could lead to local escalation of	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228314987 **CVE ID : CVE-2022-20360**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	10-Aug-2022	7	In stealReceiveChannel of EventThread.cpp, there is a possible way to interfere with process communication due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-232541124 **CVE ID : CVE-2022-20344**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2440
Out-of-bounds Read	10-Aug-2022	6.5	In updateAudioTrackInfoFromESDS_MPEG4Audio of MPEG4Extractor.cpp, there is a possible	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-230493653 **CVE ID : CVE-2022-20346**		
Improper Input Validation	10-Aug-2022	5.5	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible way to trick the victim to grant notification access to the wrong app due to improper input validation. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228178437 **CVE ID : CVE-2022-20350**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	10-Aug-2022	5.5	In addProviderRequestListener of LocationManagerService.java, there is a possible way to learn which packages request location information due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-222473855 **CVE ID : CVE-2022-20352**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2443
Improper Input Validation	10-Aug-2022	5.5	In onSaveRingtone of DefaultRingtonePreference.java, there is a possible inappropriate file read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-12LAndroid ID: A-221041256 **CVE ID : CVE-2022-20353**		
Improper Input Validation	10-Aug-2022	5.5	In get of PacProxyService.java , there is a possible system service crash due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-219498290 **CVE ID : CVE-2022-20355**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2445
Missing Initialization of Resource	10-Aug-2022	5.5	In writeToParcel of SurfaceControl.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-214999987	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20357		
Incorrect Default Permissions	10-Aug-2022	3.3	In startSync of AbstractThreadedSyncAdapter.java, there is a possible way to access protected content of content providers due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-203229608 **CVE ID : CVE-2022-20358**	https://source.android.com/security/bulletin/2022-08-01	O-GOO-ANDR-180822/2447
Affected Version(s): 13.0					
N/A	12-Aug-2022	7.8	In Settings, there is a possible way to bypass factory reset protections due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-201561699 **CVE ID : CVE-2022-20297**		
N/A	12-Aug-2022	7.8	In Bluetooth, there is a possible way to bypass compiler exploit mitigations due to a configuration error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-221893030 **CVE ID : CVE-2022-20258**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2449
Improper Privilege Management	12-Aug-2022	7.8	In RestrictionsManager, there is a possible way to send a broadcast that should be restricted to system apps due to a permissions bypass. This could lead to local escalation of privilege on an enterprise managed device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-210468836 **CVE ID : CVE-2022-20268**		
N/A	12-Aug-2022	7.8	In Settings, there is a possible way to bypass factory reset protections due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-202975040 **CVE ID : CVE-2022-20292**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2451
N/A	12-Aug-2022	7.6	In Settings, there is a possible way to bypass factory reset protections due to a sandbox escape. This could lead to local escalation of privilege if the attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200746457	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20302		
N/A	12-Aug-2022	7.5	In hostapd, there is a possible insecure configuration due to an insecure default value. This could lead to remote denial of service of the wifi hotspot with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-197874458 **CVE ID : CVE-2022-20308**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2453
Out-of-bounds Write	12-Aug-2022	6.8	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-192206329 **CVE ID : CVE-2022-20313**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2454
Use After Free	12-Aug-2022	6.7	In Camera Provider HAL, there is a possible memory corruption due to a	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-199680794 **CVE ID : CVE-2022-20306**		
Improper Input Validation	12-Aug-2022	6.7	In KeyChain, there is a possible spoof keychain chooser activity request 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.Product: AndroidVersions: Android-13Android ID: A-191876118 **CVE ID : CVE-2022-20314**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2456
Out-of-bounds Write	12-Aug-2022	6.4	In the Audio HAL, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed.	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222572821 **CVE ID : CVE-2022-20256**		
Incorrect Default Permissions	12-Aug-2022	5.5	In Content, there is a possible way to check if an account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200956614 **CVE ID : CVE-2022-20301**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2458
Incorrect Default Permissions	12-Aug-2022	5.5	In Telephony, there is a possible leak of ICCID and EID due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-221431393 **CVE ID : CVE-2022-20259**		
Uncontrolled Resource Consumption	12-Aug-2022	5.5	In the Phone app, there is a possible crash loop due to resource exhaustion. This could lead to local persistent denial of service in the Phone app with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-220865698 **CVE ID : CVE-2022-20260**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2460
Incorrect Default Permissions	12-Aug-2022	5.5	In Content, there is a possible way to check if the given account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200956588 **CVE ID : CVE-2022-20300**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	12-Aug-2022	5.5	In ContentService, there is a possible way to check if the given account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201415895 **CVE ID : CVE-2022-20299**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2462
Incorrect Default Permissions	12-Aug-2022	5.5	In ActivityManager, there is a way to read process state for other users due to a missing permission check. This could lead to local information disclosure of app usage with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-217935264 **CVE ID : CVE-2022-20263**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2463
Incorrect Default	12-Aug-2022	5.5	In ContentService, there is a possible way to check if an	https://source.android.com/s	O-GOO-ANDR-180822/2464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201416182 **CVE ID : CVE-2022-20298**	ecurity/bulletin/android-13	
Observable Discrepancy	12-Aug-2022	5.5	In AppOpsService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-203430648 **CVE ID : CVE-2022-20291**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2465
Observable Discrepancy	12-Aug-2022	5.5	In LauncherApps, there is a possible way to determine whether an app is	https://source.android.com/s	O-GOO-ANDR-180822/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-202298672 **CVE ID : CVE-2022-20293**	ecurity/bulleti n/android-13	
Incorrect Default Permissions	12-Aug-2022	5.5	In Content, there is a possible way to learn about an account present on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-202160705 **CVE ID : CVE-2022-20294**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2467
Incorrect Default Permissions	12-Aug-2022	5.5	In ContentService, there is a possible way to check if an account exists on the device due to a	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-202160584 **CVE ID : CVE-2022-20295**		
Incorrect Default Permissions	12-Aug-2022	5.5	In ContentService, there is a possible way to check if an account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201794303 **CVE ID : CVE-2022-20296**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2469
Incorrect Default Permissions	12-Aug-2022	5.5	In ContentService, there is a possible way to determine if an account is on the device without GET_ACCOUNTS permission due to a missing permission	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200573021 **CVE ID : CVE-2022-20303**		
Observable Discrepancy	12-Aug-2022	5.5	In Content, there is a possible way to determinate the user's account due to side channel information disclosure. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-199751919 **CVE ID : CVE-2022-20304**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2471
Incorrect Default Permissions	12-Aug-2022	5.5	In WifiP2pManager, there is a possible toobtain WiFi P2P MAC address without user consent due to missing permission check. This could lead to local information	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure without additional execution privileges needed. User interaction is not needed forexploitationProduct: AndroidVersions: Android-13Android ID: A-192244925 **CVE ID : CVE-2022-20312**		
Improper Input Validation	12-Aug-2022	5	In Companion, there is a possible way to keep a service running with elevated importance without showing foreground service notification due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-211757348 **CVE ID : CVE-2022-20266**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2473
Improper Privilege Management	12-Aug-2022	4.6	In Settings, there is a possible way to bypass factory reset permissions due to a permissions bypass. This could lead to local escalation of privilege with physical access to	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-212804898 **CVE ID : CVE-2022-20265**		
Incorrect Default Permissions	12-Aug-2022	4.4	In SettingsProvider, there is a possible way to read or change the default ringtone due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222687217 **CVE ID : CVE-2022-20255**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2475
N/A	12-Aug-2022	3.3	In Bluetooth, there is a possible way to pair a display only device without PIN confirmation due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222289114 **CVE ID : CVE-2022-20257**		
Observable Discrepancy	12-Aug-2022	3.3	In AlarmManagerService, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-198782887 **CVE ID : CVE-2022-20307**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2477
Incorrect Default Permissions	12-Aug-2022	3.3	In bluetooth, there is a possible way to enable or disable bluetooth connection without user consent due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-211646835 **CVE ID : CVE-2022-20267**		
Observable Discrepancy	12-Aug-2022	3.3	In PackageInstaller, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-194694094 **CVE ID : CVE-2022-20309**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2479
Incorrect Default Permissions	12-Aug-2022	3.3	In Telecomm, there is a possible disclosure of registered self managed phone accounts due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-192663798 **CVE ID : CVE-2022-20310**		
Incorrect Default Permissions	12-Aug-2022	3.3	In Telecomm, there is a possible disclosure of registered self managed phone accounts due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-192663553 **CVE ID : CVE-2022-20311**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2481
Incorrect Permission Assignment for Critical Resource	12-Aug-2022	3.3	In ActivityManager, there is a possible way to check another process's capabilities due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-218338453 **CVE ID : CVE-2022-20262**		
Incorrect Default Permissions	12-Aug-2022	3.3	In ContentService, there is a possible disclosure of available account types due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-199751623 **CVE ID : CVE-2022-20305**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2483
Incorrect Default Permissions	12-Aug-2022	3.3	In ActivityManager, there is a possible disclosure of installed packages due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-191058227	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20315		
Observable Discrepancy	12-Aug-2022	3.3	In ContentResolver, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-190726121 **CVE ID : CVE-2022-20316**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2485
Incorrect Default Permissions	12-Aug-2022	2.3	In LocationManager, there is a possible way to get location information due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-219835125	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20261		
Affected Version(s): 13.0.0					
Incorrect Default Permissions	11-Aug-2022	7.8	In WindowManager, there is a possible bypass of the restrictions for starting activities from the background due to an incorrect UID/permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-230493191 **CVE ID : CVE-2022-20246**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2487
N/A	11-Aug-2022	7.8	In Settings, there is a possible way to connect to an open network bypassing DISALLOW_CONFIG_WIFI restriction due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-227619193 **CVE ID : CVE-2022-20248**		
Improper Input Validation	11-Aug-2022	7.8	In Messaging, there is a possible way to attach files to a message without proper access checks due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226134095 **CVE ID : CVE-2022-20250**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2489
Out-of-bounds Write	11-Aug-2022	7.5	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if more than 100 bluetooth devices have been connected with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-201083240 **CVE ID : CVE-2022-20244**		
Out-of-bounds Write	11-Aug-2022	7.5	In Media, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-229858836 **CVE ID : CVE-2022-20247**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2491
Observable Discrepancy	11-Aug-2022	5.5	In Telephony, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-231986212	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20242		
Cleartext Transmission of Sensitive Information	11-Aug-2022	4.4	In Core Utilities, there is a possible log information disclosure. This could lead to local information disclosure of sensitive browsing data with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-190199986 **CVE ID : CVE-2022-20243**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2493
Improper Input Validation	11-Aug-2022	3.3	In Messaging, there is a possible way to attach a private file to an SMS message due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-217185011 **CVE ID : CVE-2022-20241**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	11-Aug-2022	3.3	In LocaleManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226900861 **CVE ID : CVE-2022-20249**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2495
Observable Discrepancy	11-Aug-2022	3.3	In LocaleManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-225881167	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20251		
Observable Discrepancy	11-Aug-2022	3.3	In PackageManager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-224547584 **CVE ID : CVE-2022-20252**	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2497
N/A	11-Aug-2022	2.4	In WindowManager, there is a possible method to create a recording of the lock screen due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-215005011	https://source.android.com/security/bulletin/android-13	O-GOO-ANDR-180822/2498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20245		
Product: chrome_os					
Affected Version(s): -					
Out-of-bounds Write	12-Aug-2022	9.8	Out of bounds write in Chrome OS Audio Server in Google Chrome on Chrome OS prior to 102.0.5005.125 allowed a remote attacker to potentially exploit heap corruption via crafted audio metadata. **CVE ID : CVE-2022-2587**	https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-chromeos.html, https://crbug.com/1320917	O-GOO-CHRO-180822/2499
Use After Free	12-Aug-2022	8.8	Use after free in Tab Strip in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2607**	https://crbug.com/1286203, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	O-GOO-CHRO-180822/2500
Use After Free	12-Aug-2022	8.8	Use after free in Nearby Share in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html,	O-GOO-CHRO-180822/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2609**	https://crbug.com/1338560	
Use After Free	12-Aug-2022	8.8	Use after free in Input in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to enage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2613**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1325256	O-GOO-CHRO-180822/2502
Use After Free	12-Aug-2022	8.8	Use after free in WebUI in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions. **CVE ID : CVE-2022-2620**	https://crbug.com/1337304, https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html	O-GOO-CHRO-180822/2503
Vendor: Huawei					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: emui					
Affected Version(s): 10.0.0					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2504
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2505
Affected Version(s): 10.1.0					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387	O-HUA-EMUI-180822/2506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			up windows or run in the background. **CVE ID : CVE-2022-37002**	6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2507
Affected Version(s): 10.1.1					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2508
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-EMUI-180822/2509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	phones-202208-000000136387 6177, https://consu mer.huawei.co m/en/support/ bulletin/2022/ 8/	
Improper Neutralizat ion of Argument Delimiters in a Command ('Argument Injection')	10-Aug-2022	7.5	The Settings application has an argument injection vulnerability. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-37005**	https://device. harmonyos.co m/en/docs/sec urity/update/s ecurity-bulletins-phones-202208-000000136387 6177, https://consu mer.huawei.co m/en/support/ bulletin/2022/ 8/	O-HUA-EMUI-180822/2510
Affected Version(s): 11.0.0					
Incorrect Authorizati on	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device. harmonyos.co m/en/docs/sec urity/update/s ecurity-bulletins-phones-202208-000000136387 6177, https://consu mer.huawei.co m/en/support/ bulletin/2022/ 8/	O-HUA-EMUI-180822/2511
Incorrect Default	10-Aug-2022	9.8	The AOD module has a vulnerability in permission	https://device. harmonyos.co m/en/docs/sec	O-HUA-EMUI-180822/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			assignment. Successful exploitation of this vulnerability may cause permission escalation and unauthorized access to files. **CVE ID : CVE-2022-37003**	urity/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2513
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	10-Aug-2022	7.5	The Settings application has an argument injection vulnerability. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-37005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	10-Aug-2022	7.5	The chinadrm module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37007**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2515
Insufficient Verification of Data Authenticity	10-Aug-2022	7.5	The recovery module has a vulnerability of bypassing the verification of an update package before use. Successful exploitation of this vulnerability may affect system stability. **CVE ID : CVE-2022-37008**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2516
Affected Version(s): 11.0.1					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.co	O-HUA-EMUI-180822/2517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37002	m/en/support/bulletin/2022/8/	
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2518
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	10-Aug-2022	7.5	The Settings application has an argument injection vulnerability. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-37005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2519
Insufficient Verification of Data Authenticity	10-Aug-2022	7.5	The recovery module has a vulnerability of bypassing the verification of an update package before use. Successful exploitation of this vulnerability may	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177,	O-HUA-EMUI-180822/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affect system stability. **CVE ID : CVE-2022-37008**	https://consumer.huawei.com/en/support/bulletin/2022/8/	
Affected Version(s): 12.0.0					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2521
Incorrect Default Permissions	10-Aug-2022	9.8	The AOD module has a vulnerability in permission assignment. Successful exploitation of this vulnerability may cause permission escalation and unauthorized access to files. **CVE ID : CVE-2022-37003**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2522
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-	O-HUA-EMUI-180822/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	10-Aug-2022	7.5	The Settings application has an argument injection vulnerability. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-37005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2524
Incorrect Default Permissions	10-Aug-2022	7.5	Permission control vulnerability in the network module. Successful exploitation of this vulnerability may affect service availability. **CVE ID : CVE-2022-37006**	https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2525
Out-of-bounds Read	10-Aug-2022	7.5	The chinadrm module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect the availability.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177,	O-HUA-EMUI-180822/2526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37007	https://consumer.huawei.com/en/support/bulletin/2022/8/	
Insufficient Verification of Data Authenticity	10-Aug-2022	7.5	The recovery module has a vulnerability of bypassing the verification of an update package before use. Successful exploitation of this vulnerability may affect system stability. **CVE ID : CVE-2022-37008**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-EMUI-180822/2527
Product: harmonyos					
Affected Version(s): 2.0					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-HARM-180822/2528
Incorrect Default Permissions	10-Aug-2022	9.8	The AOD module has a vulnerability in permission assignment. Successful	https://device.harmonyos.com/en/docs/security/update/security-	O-HUA-HARM-180822/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may cause permission escalation and unauthorized access to files. **CVE ID : CVE-2022-37003**	bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	
N/A	10-Aug-2022	7.5	The diag-router module has a vulnerability in intercepting excessive long and short instructions. Successful exploitation of this vulnerability will cause the diag-router module to crash. **CVE ID : CVE-2022-37001**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177	O-HUA-HARM-180822/2530
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-HARM-180822/2531
Improper Neutralization of Argument Delimiters	10-Aug-2022	7.5	The Settings application has an argument injection vulnerability. Successful	https://device.harmonyos.com/en/docs/security/update/security-	O-HUA-HARM-180822/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
in a Command ('Argument Injection')			exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-37005**	bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	
Out-of-bounds Read	10-Aug-2022	7.5	The chinadrm module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37007**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-HARM-180822/2533
Insufficient Verification of Data Authenticity	10-Aug-2022	7.5	The recovery module has a vulnerability of bypassing the verification of an update package before use. Successful exploitation of this vulnerability may affect system stability. **CVE ID : CVE-2022-37008**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-HARM-180822/2534
Product: magic_ui					
Affected Version(s): 3.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-MAGI-180822/2535
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-MAGI-180822/2536
Affected Version(s): 3.1.0					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.co	O-HUA-MAGI-180822/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-37002	m/en/support/bulletin/2022/8/	
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-0000001363876177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-MAGI-180822/2538
Affected Version(s): 3.1.1					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-0000001363876177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-MAGI-180822/2539
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387	O-HUA-MAGI-180822/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	10-Aug-2022	7.5	The Settings application has an argument injection vulnerability. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-37005**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-MAGI-180822/2541
Affected Version(s): 4.0.0					
Incorrect Authorization	10-Aug-2022	9.8	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background. **CVE ID : CVE-2022-37002**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-MAGI-180822/2542
Incorrect Default Permissions	10-Aug-2022	9.8	The AOD module has a vulnerability in permission assignment. Successful exploitation of this	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-MAGI-180822/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause permission escalation and unauthorized access to files. **CVE ID : CVE-2022-37003**	phones-202208-000000136387 6177, https://consu mer.huawei.co m/en/support/ bulletin/2022/ 8/	
N/A	10-Aug-2022	7.5	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37004**	https://device. harmonyos.co m/en/docs/sec urity/update/s ecurity-bulletins-phones-202208-000000136387 6177, https://consu mer.huawei.co m/en/support/ bulletin/2022/ 8/	O-HUA-MAGI-180822/2544
Improper Neutralizat ion of Argument Delimiters in a Command ('Argument Injection')	10-Aug-2022	7.5	The Settings application has an argument injection vulnerability. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-37005**	https://device. harmonyos.co m/en/docs/sec urity/update/s ecurity-bulletins-phones-202208-000000136387 6177, https://consu mer.huawei.co m/en/support/ bulletin/2022/ 8/	O-HUA-MAGI-180822/2545
Out-of-bounds Read	10-Aug-2022	7.5	The chinadrm module has an out-of-bounds read vulnerability.	https://device. harmonyos.co m/en/docs/sec urity/update/s	O-HUA-MAGI-180822/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability may affect the availability. **CVE ID : CVE-2022-37007**	ecurity-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	
Insufficient Verification of Data Authenticity	10-Aug-2022	7.5	The recovery module has a vulnerability of bypassing the verification of an update package before use. Successful exploitation of this vulnerability may affect system stability. **CVE ID : CVE-2022-37008**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-000000136387 6177, https://consumer.huawei.com/en/support/bulletin/2022/8/	O-HUA-MAGI-180822/2547
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	10-Aug-2022	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in a stack trace. This information could be used in further attacks against the	https://exchange.xforce.ibmcloud.com/vulnerabilities/231202, https://www.ibm.com/support/pages/node/6610883	O-IBM-AIX-180822/2548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X-Force ID: 231202. **CVE ID : CVE-2022-35715**		
Product: mq_appliance_m2001_firmware					
Affected Version(s): * Up to (excluding) 9.2.0.5					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	O-IBM-MQ_A-180822/2549
Affected Version(s): * Up to (excluding) 9.2.5					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	O-IBM-MQ_A-180822/2550
Product: mq_appliance_m2002_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 9.2.0.5					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	O-IBM-MQ_A-180822/2551
Affected Version(s): * Up to (excluding) 9.2.5					
Incorrect Authorization	01-Aug-2022	3.3	IBM Datapower Gateway 10.0.2.0 through 10.0.4.0, 10.0.1.0 through 10.0.1.5, and 2018.4.1.0 through 2018.4.1.18 could allow unauthorized viewing of logs and files due to insufficient authorization checks. IBM X-Force ID: 218856. **CVE ID : CVE-2022-22326**	https://www.ibm.com/support/pages/node/6560048, https://www.ibm.com/support/pages/node/6608598, https://exchange.xforce.ibmcloud.com/vulnerabilities/218856	O-IBM-MQ_A-180822/2552
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation	https://www.vmware.com/security/advisories/VMSA-	O-LIN-LINU-180822/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	2022-0021.html	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-LIN-LINU-180822/2554
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-LIN-LINU-180822/2555
Improper Privilege	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity	https://www.vmware.com/se	O-LIN-LINU-180822/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	curity/advisories/VMSA-2022-0021.html	
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-LIN-LINU-180822/2557
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-LIN-LINU-180822/2558
Generation of Error Message Containing Sensitive	10-Aug-2022	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive	https://exchange.xforce.ibmcloud.com/vulnerabilities/231202,	O-LIN-LINU-180822/2559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			information when a detailed technical error message is returned in a stack trace. This information could be used in further attacks against the system. IBM X-Force ID: 231202. **CVE ID : CVE-2022-35715**	https://www.ibm.com/support/pages/node/6610883	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-LIN-LINU-180822/2560
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-LIN-LINU-180822/2561
Improper Neutralization of	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and	https://www.vmware.com/security/advisori	O-LIN-LINU-180822/2562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements in Output Used by a Downstream Component ('Injection')			vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	es/VMSA-2022-0021.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-LIN-LINU-180822/2563
Affected Version(s): * Up to (excluding) 4.7					
N/A	10-Aug-2022	6.5	Linux deployments of StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.2 deployed with a Linux kernel version less than 4.7.0 are susceptible to a vulnerability	https://security.netapp.com/advisory/NTAP-20220808-0001/	O-LIN-LINU-180822/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could allow a remote unauthenticated attacker to view limited metrics information and modify alert email recipients and content. **CVE ID : CVE-2022-23238**		
Affected Version(s): * Up to (excluding) 5.18					
Missing Release of Memory after Effective Lifetime	05-Aug-2022	9.1	A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table perturb size. This flaw may allow an attacker to information leak and may cause a denial of service problem. **CVE ID : CVE-2022-1012**	https://kernel.googlesource.com/pub/scm/linux/kernel/git/jkirsher/net-queue/+/b2d057560b8107c633b39aabe517ff9d93f285e3%5E%21/	O-LIN-LINU-180822/2565
Affected Version(s): * Up to (excluding) 5.19					
Use After Free	05-Aug-2022	7.1	A use-after-free flaw was found in the Linux kernel in log_replay in fs/ntfs3/fslog.c in the NTFS journal. This flaw allows a local attacker to crash the system and leads to a kernel information leak problem.	N/A	O-LIN-LINU-180822/2566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-1973		
Affected Version(s): 5.18					
Missing Release of Memory after Effective Lifetime	05-Aug-2022	9.1	A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table perturb size. This flaw may allow an attacker to information leak and may cause a denial of service problem. **CVE ID : CVE-2022-1012**	https://kernel.googlesource.com/pub/scm/linux/kernel/git/jkirsher/net-queue/+/b2d057560b8107c633b39aabe517ff9d93f285e3%5E%21/	O-LIN-LINU-180822/2567
Affected Version(s): From (including) 5.2 Up to (excluding) 5.18					
Use After Free	05-Aug-2022	7.8	A flaw was found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the offset to get the page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition. **CVE ID : CVE-2022-1158**	N/A	O-LIN-LINU-180822/2568
Vendor: mediatek					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: mt7603_firmware					
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2569
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2570
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-MED-MT76-180822/2571

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2572
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	O-MED-MT76-180822/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2574
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26444		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2576
Product: mt7610_firmware					
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2578
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2579
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	O-MED-MT76-180822/2580

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: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2581
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2583
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2584
Product: mt7612_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2585
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2586
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2587

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2588
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due 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/August-2022	O-MED-MT76-180822/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2590
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2592
Product: mt7613_firmware					
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2593
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-MED-MT76-180822/2594

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: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2595
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	O-MED-MT76-180822/2596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2597
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26443		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2599
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2600
Product: mt7615_firmware					
Affected Version(s): 7.6.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2601
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2602
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	O-MED-MT76-180822/2603

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2604
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2606
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2608
Product: mt7620_firmware					
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2609
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-MED-MT76-180822/2610

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: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2611
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	O-MED-MT76-180822/2612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2613
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26443		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2615
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2616
Product: mt7622_firmware					
Affected Version(s): 7.6.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2617
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2618
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	O-MED-MT76-180822/2619

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2620
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2622
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2624
Product: mt7628_firmware					
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2625
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-MED-MT76-180822/2626

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: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2627
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	O-MED-MT76-180822/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2629
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26443		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2631
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2632
Product: mt7629_firmware					
Affected Version(s): 7.6.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2633
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2634
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	O-MED-MT76-180822/2635

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2636
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2638
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT76-180822/2640
Product: mt7915_firmware					
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2641
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-MED-MT79-180822/2642

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: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2643
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	O-MED-MT79-180822/2644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2645
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26443		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2647
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2648
Product: mt7916_firmware					
Affected Version(s): 7.6.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2649
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2650
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	O-MED-MT79-180822/2651

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2652
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2654
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2656
Product: mt7986_firmware					
Affected Version(s): 7.6.2.3					
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2657
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-MED-MT79-180822/2658

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: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	bulletin/August-2022	
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2659
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of 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/August-2022	O-MED-MT79-180822/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051; Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2661
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068.	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26443		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2663
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT79-180822/2664
Product: mt8981_firmware					
Affected Version(s): 7.6.2.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420013; Issue ID: GN20220420013. **CVE ID : CVE-2022-26438**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT89-180822/2665
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420020; Issue ID: GN20220420020. **CVE ID : CVE-2022-26439**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT89-180822/2666
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, 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/August-2022	O-MED-MT89-180822/2667

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: GN20220420037; Issue ID: GN20220420037. **CVE ID : CVE-2022-26440**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420044; Issue ID: GN20220420044. **CVE ID : CVE-2022-26441**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT89-180822/2668
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420051;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT89-180822/2669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: GN20220420051. **CVE ID : CVE-2022-26442**		
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420068; Issue ID: GN20220420068. **CVE ID : CVE-2022-26443**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT89-180822/2670
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420075; Issue ID: GN20220420075. **CVE ID : CVE-2022-26444**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT89-180822/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In wifi driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: GN20220420088; Issue ID: GN20220420088. **CVE ID : CVE-2022-26445**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-MED-MT89-180822/2672
Vendor: megatech					
Product: msnswitch_firmware					
Affected Version(s): mnt.2408					
Improper Authentication	10-Aug-2022	9.8	An authentication-bypass issue in the component http://MYDEVICEIP/cgi-bin-sdb/ExportSettings.sh of Mega System Technologies Inc MSNSwitch MNT.2408 allows unauthenticated attackers to arbitrarily configure settings within the application, leading to remote code execution. **CVE ID : CVE-2022-32429**	N/A	O-MEG-MSNS-180822/2673
Vendor: Microsoft					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: windows					
Affected Version(s): -					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Aug-2022	9.8	Shescape is a simple shell escape package for JavaScript. Versions prior to 1.5.8 were found to be subject to code injection on windows. This impacts users that use Shescape (any API function) to escape arguments for cmd.exe on Windows An attacker can omit all arguments following their input by including a line feed character (`'\n'`) in the payload. This bug has been patched in [v1.5.8] which you can upgrade to now. No further changes are required. Alternatively, line feed characters (`'\n'`) can be stripped out manually or the user input can be made the last argument (this only limits the impact). **CVE ID : CVE-2022-31179**	https://github.com/ericcornelissen/shescape/security/advisories/GHSA-jjc5-fp7p-6f8w, https://github.com/ericcornelissen/shescape/pull/332	O-MIC-WIND-180822/2674
Improper Authentication	05-Aug-2022	9.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an	https://www.vmware.com/security/advisories/VMSA-	O-MIC-WIND-180822/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate. **CVE ID : CVE-2022-31656**	2022-0021.html	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	9.8	VMware Workspace ONE Access and Identity Manager contain a URL injection vulnerability. A malicious actor with network access may be able to redirect an authenticated user to an arbitrary domain. **CVE ID : CVE-2022-31657**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-MIC-WIND-180822/2676
Weak Password Requirements	10-Aug-2022	9.8	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 230634. **CVE ID : CVE-2022-35280**	https://www.ibm.com/support/pages/node/6610393	O-MIC-WIND-180822/2677
Improper Privilege	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and	https://www.vmware.com/security/advisori	O-MIC-WIND-180822/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			vRealize Automation contain a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31664**	es/VMSA-2022-0021.html	
Out-of-bounds Write	02-Aug-2022	7.8	The NHI card's web service component has a stack-based buffer overflow vulnerability due to insufficient validation for network packet header length. A local area network attacker with general user privilege can exploit this vulnerability to execute arbitrary code, manipulate system command or disrupt service. **CVE ID : CVE-2022-35217**	N/A	O-MIC-WIND-180822/2679
Use After Free	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	O-MIC-WIND-180822/2680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34263**		
N/A	05-Aug-2022	7.8	Kaspersky VPN Secure Connection for Windows version up to 21.5 was vulnerable to arbitrary file deletion via abuse of its 'Delete All Service Data And Reports' feature by the local authenticated attacker. **CVE ID : CVE-2022-27535**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#050822, https://forum.kaspersky.com/topic/kaspersky-statement-on-cve-2022-27535-26742/	O-MIC-WIND-180822/2681
Out-of-bounds Write	11-Aug-2022	7.8	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34260**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	O-MIC-WIND-180822/2682
Improper Privilege	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and	https://www.vmware.com/security/advisori	O-MIC-WIND-180822/2683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			vRealize Automation contains a privilege escalation vulnerability. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31660**	es/VMSA-2022-0021.html	
Improper Privilege Management	05-Aug-2022	7.8	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two privilege escalation vulnerabilities. A malicious actor with local access can escalate privileges to 'root'. **CVE ID : CVE-2022-31661**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-MIC-WIND-180822/2684
Uncontrolled Search Path Element	11-Aug-2022	7.8	Adobe Premiere Elements version 2020v20 (and earlier) is affected by an Uncontrolled Search Path Element which could lead to Privilege Escalation. An attacker could leverage this vulnerability to obtain admin using an existing low-privileged user. Exploitation of this issue does not require user interaction.	https://helpx.adobe.com/security/products/premiere_elements/apsb22-43.html	O-MIC-WIND-180822/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34235		
Out-of-bounds Read	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35673**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	O-MIC-WIND-180822/2686
Out-of-bounds Read	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	O-MIC-WIND-180822/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2022-35674**		
Use After Free	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35675**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	O-MIC-WIND-180822/2688
Heap-based Buffer Overflow	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	O-MIC-WIND-180822/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2022-35676**		
Heap-based Buffer Overflow	11-Aug-2022	7.8	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-35677**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	O-MIC-WIND-180822/2690
Generation of Error Message Containing Sensitive Information	10-Aug-2022	7.5	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in a stack trace. This information could be	https://exchange.xforce.ibmcloud.com/vulnerabilities/231202, https://www.ibm.com/support/pages/node/6610883	O-MIC-WIND-180822/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used in further attacks against the system. IBM X-Force ID: 231202. **CVE ID : CVE-2022-35715**		
NULL Pointer Dereference	06-Aug-2022	7.5	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow a NULL pointer dereference when this.Span is used for oState of Collab.addStateModel, because this.Span.text can be NULL. **CVE ID : CVE-2022-26979**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180822/2692
NULL Pointer Dereference	06-Aug-2022	7.5	Foxit PDF Reader before 12.0.1 and PDF Editor before 12.0.1 allow an exportXFAData NULL pointer dereference. **CVE ID : CVE-2022-27944**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-180822/2693
N/A	05-Aug-2022	7.5	A Denial-of-Service vulnerability was discovered in the F-Secure Atlant and in certain WithSecure products while scanning fuzzed PE32-bit files it is possible that can crash the scanning engine. The exploit can be triggered remotely by an attacker.	https://www.f-secure.com/en/home/support/vulnerability-reward-program/hall-of-fame, https://www.withsecure.com/en/expertise/people	O-MIC-WIND-180822/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-28880		
N/A	10-Aug-2022	7.5	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker. **CVE ID : CVE-2022-28881**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories, https://www.withsecure.com/en/support/security-advisories	O-MIC-WIND-180822/2695
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10-Aug-2022	7.5	Incorrect conversion of certain invalid paths to valid, absolute paths in Clean in path/filepath before Go 1.17.11 and Go 1.18.3 on Windows allows potential directory traversal attack. **CVE ID : CVE-2022-29804**	https://go.googlesource.com/go/+/9cd1818a7d019c02fa4898b3e45a323e35033290, https://groups.google.com/g/golang-announce/c/TzIC9-t8Ytg/m/IWz5T6x7AAAJ, https://pkg.go.dev/vuln/GO-2022-0533, https://go.dev/cl/401595, https://go.dev/issue/52476	O-MIC-WIND-180822/2696
Improper Limitation of a Pathname	05-Aug-2022	7.5	VMware Workspace ONE Access, Identity Manager, Connectors and vRealize	https://www.vmware.com/security/advisories/VMSA-	O-MIC-WIND-180822/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Automation contain a path traversal vulnerability. A malicious actor with network access may be able to access arbitrary files. **CVE ID : CVE-2022-31662**	2022-0021.html	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31665**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-MIC-WIND-180822/2698
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-2022	7.2	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31659**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-MIC-WIND-180822/2699
Improper Neutralization of Special Elements in Output	05-Aug-2022	7.2	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a remote code execution	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-MIC-WIND-180822/2700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Used by a Downstream Component ('Injection')			vulnerability. A malicious actor with administrator and network access can trigger a remote code execution. **CVE ID : CVE-2022-31658**		
Improper Input Validation	12-Aug-2022	6.5	Insufficient validation of untrusted input in Safe Browsing in Google Chrome on Windows prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a crafted file. **CVE ID : CVE-2022-2622**	https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html, https://crbug.com/1332392	O-MIC-WIND-180822/2701
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-2022	6.1	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a reflected cross-site scripting (XSS) vulnerability. Due to improper user input sanitization, a malicious actor with some user interaction may be able to inject javascript code in the target user's window. **CVE ID : CVE-2022-31663**	https://www.vmware.com/security/advisories/VMSA-2022-0021.html	O-MIC-WIND-180822/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	11-Aug-2022	5.5	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34264**	https://helpx.adobe.com/security/products/framemaker/apsb22-42.html	O-MIC-WIND-180822/2703
Allocation of Resources Without Limits or Throttling	02-Aug-2022	5.5	The NHI card's web service component has a heap-based buffer overflow vulnerability due to insufficient validation for packet origin parameter length. A LAN attacker with general user privilege can exploit this vulnerability to disrupt service. **CVE ID : CVE-2022-35218**	N/A	O-MIC-WIND-180822/2704
Allocation of Resources Without	02-Aug-2022	5.5	The NHI card's web service component has a stack-based buffer overflow	N/A	O-MIC-WIND-180822/2705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			vulnerability due to insufficient validation for network packet key parameter. A LAN attacker with general user privilege can exploit this vulnerability to disrupt service. **CVE ID : CVE-2022-35219**		
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-34261**	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	O-MIC-WIND-180822/2706
Out-of-bounds Read	11-Aug-2022	5.5	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/illustrator/apsb22-41.html	O-MIC-WIND-180822/2707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-2022-34262**		
Files or Directories Accessible to External Parties	10-Aug-2022	4.9	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a privileged user to obtain sensitive Azure bot credential information. IBM X-Force ID: 226342. **CVE ID : CVE-2022-22490**	https://www.ibm.com/support/pages/node/6610397, https://exchange.xforce.ibmcloud.com/vulnerabilities/226342	O-MIC-WIND-180822/2708
Product: windows_10					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/2709
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34691	ory/CVE-2022-34691	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2711
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2712
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	ory/CVE-2022-35767	
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/2714
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/2715
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/2716
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	guidance/advisory/CVE-2022-34703	
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2718
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2719
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2720
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2721
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	US/security-guidance/advisory/CVE-2022-35768	
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/2723
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2724
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2725
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30144**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30144	O-MIC-WIND-180822/2726
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30194	ory/CVE-2022-30194	
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2728
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2729
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2730
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/2731
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/2732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/2733
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2734
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/2735
Affected Version(s): 1607					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/2736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30133		
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/2737
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2738
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35767		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2740
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/2741
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/2742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/2743
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/2744
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/2745
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/2746
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	ory/CVE-2022-35792	
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/2748
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2749
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2750
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2751
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-35820**	US/security-guidance/advisory/CVE-2022-35820	
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2753
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2754
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/2755
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35762	O-MIC-WIND-180822/2756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35762		
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/2757
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/2758
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30144**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30144	O-MIC-WIND-180822/2759
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/2760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2761
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2762
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2763
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/2764
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/2765
Cleartext Transmissi	09-Aug-2022	5.5	Windows Defender Credential Guard	https://portal.msrc.microsoft.	O-MIC-WIND-180822/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Sensitive Informatio n			Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	com/en-US/security-guidance/advisory/CVE-2022-34704	
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2767
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/2768
Affected Version(s): 1809					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/2770
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/2771
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35766	O-MIC-WIND-180822/2773
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2774
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**		
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/2776
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/2777
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/2778
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	US/security-guidance/advisory/CVE-2022-33670	
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2780
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/2781
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/2782
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2783
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	guidance/advisory/CVE-2022-34703	
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771. **CVE ID : CVE-2022-34705**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/2785
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2786
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2787
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2789
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/2790
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35762	O-MIC-WIND-180822/2791
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/2792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/2793
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/2794
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30144**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30144	O-MIC-WIND-180822/2795
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/2796
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP)	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	guidance/advisory/CVE-2022-34701	
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2798
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2799
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/2800
N/A	09-Aug-2022	6.1	Windows Hello Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-35797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35797	O-MIC-WIND-180822/2801
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34709	ory/CVE-2022-34709	
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34708. **CVE ID : CVE-2022-30197**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30197	O-MIC-WIND-180822/2803
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2804
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/2805
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34710		
Affected Version(s): 20h2					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/2807
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/2808
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/2809
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	ory/CVE-2022-35767	
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35766	O-MIC-WIND-180822/2811
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2813
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/2814
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/2815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35768		
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/2816
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/2817
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/2818
Concurrent Execution using Shared Resource with Improper Synchronization	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/2819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/2820
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2821
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/2822
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771. **CVE ID : CVE-2022-34705**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/2823
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2825
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2826
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2827
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2828
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/2829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35761		
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35762	O-MIC-WIND-180822/2830
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/2831
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/2832
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. **CVE ID : CVE-2022-30144**	guidance/advisory/CVE-2022-30144	
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/2834
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2835
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2836
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2837
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34690	ory/CVE-2022-34690	
N/A	09-Aug-2022	6.1	Windows Hello Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-35797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35797	O-MIC-WIND-180822/2839
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/2840
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34708. **CVE ID : CVE-2022-30197**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30197	O-MIC-WIND-180822/2841
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2842
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**		
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/2844
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34710. **CVE ID : CVE-2022-34712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34712	O-MIC-WIND-180822/2845
Affected Version(s): 21h1					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/2846
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34691	guidance/advisory/CVE-2022-34691	
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/2848
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2849
Improper Control of Generation of Code	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	ory/CVE-2022-35766	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2851
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**		
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/2853
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/2854
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/2855
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/2856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33670		
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/2857
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/2858
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/2859
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2860
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	US/security-guidance/advisory/CVE-2022-34703	
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771. **CVE ID : CVE-2022-34705**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/2862
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2863
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2864
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2865
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	US/security-guidance/advisory/CVE-2022-34713	
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2867
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/2868
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35762	O-MIC-WIND-180822/2869
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	ory/CVE-2022-35763	
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/2871
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30144**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30144	O-MIC-WIND-180822/2872
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/2873
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2874
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	US/security-guidance/advisory/CVE-2022-35769	
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2876
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/2877
N/A	09-Aug-2022	6.1	Windows Hello Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-35797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35797	O-MIC-WIND-180822/2878
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/2879
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-34708. **CVE ID : CVE-2022-30197**	ory/CVE-2022-30197	
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2881
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/2882
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/2883
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-34704, CVE-2022-34710. **CVE ID : CVE-2022-34712**	ory/CVE-2022-34712	
Affected Version(s): 21h2					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2885
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35766	O-MIC-WIND-180822/2887
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2888
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/2889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/2890
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/2891
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/2892
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/2893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34705		
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2894
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2895
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2896
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2897
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	ory/CVE-2022-35761	
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35762	O-MIC-WIND-180822/2899
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/2900
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/2901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/2902
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/2903
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/2904
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/2905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35792		
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2906
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2907
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2908
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2909
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	6.1	Windows Hello Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-35797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35797	O-MIC-WIND-180822/2911
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/2912
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/2913
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2914
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/2915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**		
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34710. **CVE ID : CVE-2022-34712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34712	O-MIC-WIND-180822/2916
Product: windows_11					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/2917
N/A	09-Aug-2022	8.8	SMB Client and Server Remote Code Execution Vulnerability. **CVE ID : CVE-2022-35804**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35804	O-MIC-WIND-180822/2918
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2920
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/2921
Concurrent Execution using Shared Resource with Improper Synchronization	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**		
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35766	O-MIC-WIND-180822/2923
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/2925
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/2926
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2927
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/2928
Concurrent Execution using Shared Resource	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			**CVE ID : CVE-2022-34696**	ory/CVE-2022-34696	
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/2930
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/2931
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771. **CVE ID : CVE-2022-34705**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/2932
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2933
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	US/security-guidance/advisory/CVE-2022-34707	
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2935
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2936
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2937
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/2938
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege	https://portal.msrc.microsoft.	O-MIC-WIND-180822/2939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	com/en-US/security-guidance/advisory/CVE-2022-35768	
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30144**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30144	O-MIC-WIND-180822/2940
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/2941
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2942
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2943
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	guidance/advisory/CVE-2022-35793	
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/2945
N/A	09-Aug-2022	6.1	Windows Hello Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-35797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35797	O-MIC-WIND-180822/2946
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/2947
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34708. **CVE ID : CVE-2022-30197**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30197	O-MIC-WIND-180822/2948
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			34704, CVE-2022-34710. **CVE ID : CVE-2022-34712**	ory/CVE-2022-34712	
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2950
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/2951
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/2952
Product: windows_7					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	guidance/advisory/CVE-2022-30133	
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/2954
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2955
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2957
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2958
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2959
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/2960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	US/security-guidance/advisory/CVE-2022-34713	
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/2961
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/2962
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2963
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2964
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. **CVE ID : CVE-2022-30194**	ory/CVE-2022-30194	
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2966
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2967
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2968
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/2969
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/2970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-30197. **CVE ID : CVE-2022-34708**	ory/CVE-2022-34708	
Product: windows_8.1					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/2971
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/2972
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2974
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2975
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/2976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-33670		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/2977
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2978
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/2979
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2980
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of	https://portal.msrc.microsoft.	O-MIC-WIND-180822/2981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-35760**	com/en-US/security-guidance/advisory/CVE-2022-35760	
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/2982
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/2983
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/2984
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30144**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30144	O-MIC-WIND-180822/2985
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/2986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-30194		
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/2987
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/2988
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/2989
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/2990
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/2991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34708		
Product: windows_rt_8.1					
Affected Version(s): -					
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/2992
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/2993
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/2995
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/2996
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/2997
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/2998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	guidance/advisory/CVE-2022-34707	
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/2999
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3000
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3001
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/3002
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/3003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability. **CVE ID : CVE-2022-35820**	US/security-guidance/advisory/CVE-2022-35820	
N/A	09-Aug-2022	7.5	Windows Bluetooth Service Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30144**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30144	O-MIC-WIND-180822/3004
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3005
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3006
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3007
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35793		
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3009
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3010
Product: windows_server_2008					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3011
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/3012
Concurrent Execution using Shared	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	guidance/advisory/CVE-2022-34702	
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/3014
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/3015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**		
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/3016
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3017
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3018
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3019
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP)	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	ory/CVE-2022-34701	
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3021
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3022
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3023
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3024
Affected Version(s): r2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3025
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/3026
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/3027
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/3028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/3029
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/3030
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34707		
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/3032
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3033
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3034
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/3035
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-35820	
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3037
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3038
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3039
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3040
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3042
Product: windows_server_2012					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3043
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/3044
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/3045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/3046
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/3047
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	guidance/advisory/CVE-2022-33670	
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/3049
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3050
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/3051
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3052
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/3053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	US/security-guidance/advisory/CVE-2022-35768	
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/3054
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/3055
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3056
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3057
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35769		
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3059
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3060
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3061
Affected Version(s): r2					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3062
N/A	09-Aug-2022	8.8	Active Directory Domain Services	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	US/security-guidance/advisory/CVE-2022-34691	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/3064
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/3065
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	guidance/advisory/CVE-2022-35767	
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/3067
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/3068
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3070
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/3071
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3072
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3073
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ory/CVE-2022-35795	
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/3075
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3076
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3077
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3078
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3080
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3081
Product: windows_server_2016					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3082
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/3083
Concurrent Execution using Shared Resource with	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	ory/CVE-2022-34702	
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/3085
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/3086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**		
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/3087
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/3088
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/3089
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/3090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/3091
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3092
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/3093
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3094
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/3095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35761		
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35762	O-MIC-WIND-180822/3096
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/3097
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/3098
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/3099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	guidance/advisory/CVE-2022-35765	
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3100
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/3101
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/3102
N/A	09-Aug-2022	7.8	Windows Error Reporting Service	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-180822/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	US/security-guidance/advisory/CVE-2022-35795	
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/3104
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3105
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3106
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3107
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35793		
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3109
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/3110
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/3111
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3112
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	ory/CVE-2022-34710	
Affected Version(s): 20h2					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3114
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/3115
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35766	O-MIC-WIND-180822/3117
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/3118
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/3119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/3120
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3121
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35771	O-MIC-WIND-180822/3122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35771		
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/3123
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/3124
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/3125
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/3126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/3127
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/3128
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771. **CVE ID : CVE-2022-34705**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/3129
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/3130
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/3132
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/3133
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3134
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/3135
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35762	O-MIC-WIND-180822/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**		
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/3137
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/3138
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3140
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3141
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3142
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3143
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3144
N/A	09-Aug-2022	6	Windows Defender Credential Guard	https://portal.msrc.microsoft.	O-MIC-WIND-180822/3145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	com/en-US/security-guidance/advisory/CVE-2022-34709	
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34708. **CVE ID : CVE-2022-30197**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30197	O-MIC-WIND-180822/3146
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3147
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/3148
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/3149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**		
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34710. **CVE ID : CVE-2022-34712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34712	O-MIC-WIND-180822/3150
Product: windows_server_2019					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3151
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/3152
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/3153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**		
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35766	O-MIC-WIND-180822/3154
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/3155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34702		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34714	O-MIC-WIND-180822/3156
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/3157
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from CVE-2022-34705. **CVE ID : CVE-2022-35771**	ory/CVE-2022-35771	
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/3159
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/3160
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/3161
Concurrent Execution using Shared Resource with Improper Synchronization	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34696	O-MIC-WIND-180822/3162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')					
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/3163
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/3164
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/3165
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771. **CVE ID : CVE-2022-34705**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/3166
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34706**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34706	O-MIC-WIND-180822/3167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3168
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/3169
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3170
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/3171
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35763, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**	ory/CVE-2022-35762	
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/3173
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/3174
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792. **CVE ID : CVE-2022-35765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/3175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3176
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3177
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3178
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3179
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755. **CVE ID : CVE-2022-35793**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3181
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/3182
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34708. **CVE ID : CVE-2022-30197**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30197	O-MIC-WIND-180822/3183
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3184
Cleartext Transmission of Sensitive Information	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34710, CVE-2022-34712.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34704	O-MIC-WIND-180822/3185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34704		
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/3186
Product: windows_server_2022					
Affected Version(s): -					
N/A	09-Aug-2022	9.8	Windows Point-to-Point Protocol (PPP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35744. **CVE ID : CVE-2022-30133**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30133	O-MIC-WIND-180822/3187
N/A	09-Aug-2022	9.8	Windows Network File System Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34715**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34715	O-MIC-WIND-180822/3188
N/A	09-Aug-2022	8.8	Active Directory Domain Services Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34691**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34691	O-MIC-WIND-180822/3189
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling	https://portal.msrc.microsoft.	O-MIC-WIND-180822/3190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34714**	com/en-US/security-guidance/advisory/CVE-2022-34714	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-34702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34702	O-MIC-WIND-180822/3191
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35767	O-MIC-WIND-180822/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35794. **CVE ID : CVE-2022-35767**		
N/A	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35766, CVE-2022-35767. **CVE ID : CVE-2022-35794**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35794	O-MIC-WIND-180822/3193
Improper Control of Generation of Code ('Code Injection')	09-Aug-2022	8.1	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-34702, CVE-2022-34714, CVE-2022-35745, CVE-2022-35752, CVE-2022-35753, CVE-2022-35767, CVE-2022-35794. **CVE ID : CVE-2022-35766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35766	O-MIC-WIND-180822/3194
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard	https://portal.msrc.microsoft.	O-MIC-WIND-180822/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34705. **CVE ID : CVE-2022-35771**	com/en-US/security-guidance/advisory/CVE-2022-35771	
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35765. **CVE ID : CVE-2022-35792**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35792	O-MIC-WIND-180822/3196
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34703. **CVE ID : CVE-2022-33670**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33670	O-MIC-WIND-180822/3197
N/A	09-Aug-2022	7.8	Windows Error Reporting Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35795**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35795	O-MIC-WIND-180822/3198
Concurrent Execution using Shared Resource with Improper	09-Aug-2022	7.8	Windows Hyper-V Remote Code Execution Vulnerability. **CVE ID : CVE-2022-34696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')				ory/CVE-2022-34696	
N/A	09-Aug-2022	7.8	Windows Win32k Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34699**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34699	O-MIC-WIND-180822/3200
N/A	09-Aug-2022	7.8	Windows Bluetooth Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35820**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35820	O-MIC-WIND-180822/3201
N/A	09-Aug-2022	7.8	Windows Partition Management Driver Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-33670. **CVE ID : CVE-2022-34703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34703	O-MIC-WIND-180822/3202
N/A	09-Aug-2022	7.8	Windows Defender Credential Guard Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35771. **CVE ID : CVE-2022-34705**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34705	O-MIC-WIND-180822/3203
N/A	09-Aug-2022	7.8	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability.	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-34706	ory/CVE-2022-34706	
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35761, CVE-2022-35768. **CVE ID : CVE-2022-34707**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34707	O-MIC-WIND-180822/3205
N/A	09-Aug-2022	7.8	Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-35743. **CVE ID : CVE-2022-34713**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34713	O-MIC-WIND-180822/3206
N/A	09-Aug-2022	7.8	Microsoft ATA Port Driver Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-35760**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35760	O-MIC-WIND-180822/3207
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35768. **CVE ID : CVE-2022-35761**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35761	O-MIC-WIND-180822/3208
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-180822/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2022-35763, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35762**	guidance/advisory/CVE-2022-35762	
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35764, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35763	O-MIC-WIND-180822/3210
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35765, CVE-2022-35792. **CVE ID : CVE-2022-35764**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35764	O-MIC-WIND-180822/3211
N/A	09-Aug-2022	7.8	Storage Spaces Direct Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35762, CVE-2022-35763, CVE-2022-35764, CVE-2022-35792.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35765	O-MIC-WIND-180822/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35765		
N/A	09-Aug-2022	7.8	Windows Kernel Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-34707, CVE-2022-35761. **CVE ID : CVE-2022-35768**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35768	O-MIC-WIND-180822/3213
N/A	09-Aug-2022	7.5	Windows WebBrowser Control Remote Code Execution Vulnerability. **CVE ID : CVE-2022-30194**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30194	O-MIC-WIND-180822/3214
N/A	09-Aug-2022	7.5	Windows Secure Socket Tunneling Protocol (SSTP) Denial of Service Vulnerability. **CVE ID : CVE-2022-34701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34701	O-MIC-WIND-180822/3215
N/A	09-Aug-2022	7.5	Windows Point-to-Point Protocol (PPP) Denial of Service Vulnerability. This CVE ID is unique from CVE-2022-35747. **CVE ID : CVE-2022-35769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35769	O-MIC-WIND-180822/3216
N/A	09-Aug-2022	7.3	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-35755.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35793	O-MIC-WIND-180822/3217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35793		
N/A	09-Aug-2022	7.1	Windows Fax Service Elevation of Privilege Vulnerability. **CVE ID : CVE-2022-34690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34690	O-MIC-WIND-180822/3218
N/A	09-Aug-2022	6	Windows Defender Credential Guard Security Feature Bypass Vulnerability. **CVE ID : CVE-2022-34709**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34709	O-MIC-WIND-180822/3219
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34708. **CVE ID : CVE-2022-30197**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30197	O-MIC-WIND-180822/3220
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34712. **CVE ID : CVE-2022-34710**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34710	O-MIC-WIND-180822/3221
Cleartext Transmission of Sensitive	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique	https://portal.msrc.microsoft.com/en-US/security-guidance/advis	O-MIC-WIND-180822/3222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			from CVE-2022-34710, CVE-2022-34712. **CVE ID : CVE-2022-34704**	ory/CVE-2022-34704	
N/A	09-Aug-2022	5.5	Windows Kernel Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30197. **CVE ID : CVE-2022-34708**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34708	O-MIC-WIND-180822/3223
N/A	09-Aug-2022	5.5	Windows Defender Credential Guard Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-34704, CVE-2022-34710. **CVE ID : CVE-2022-34712**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-34712	O-MIC-WIND-180822/3224
Vendor: Paloaltonetworks					
Product: pan-os					
Affected Version(s): From (including) 10.0 Up to (excluding) 10.0.11-h1					
Uncontrolled Resource Consumption	10-Aug-2022	8.6	A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto	https://security.paloaltonetworks.com/CVE-2022-0028	O-PAL-PAN--180822/3225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Networks PA-Series (hardware), VM-Series (virtual) and CN-Series (container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering profile with one or more blocked categories assigned to a source zone that has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expected to be released no later than the week of August 15, 2022. This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers and no additional action is required from them. **CVE ID : CVE-2022-0028**		
Affected Version(s): From (including) 10.1 Up to (excluding) 10.1.6-h6					
Uncontrolled Resource Consumption	10-Aug-2022	8.6	A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto Networks PA-Series (hardware), VM-Series (virtual) and CN-Series (container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering	https://security.paloaltonetworks.com/CVE-2022-0028	O-PAL-PAN--180822/3226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			profile with one or more blocked categories assigned to a source zone that has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are expected to be released no later than the week of August 15, 2022. This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and no additional action is required from them. **CVE ID : CVE-2022-0028**		
Affected Version(s): From (including) 10.2 Up to (excluding) 10.2.2-h2					
Uncontrolled Resource Consumption	10-Aug-2022	8.6	A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto Networks PA-Series (hardware), VM-Series (virtual) and CN-Series (container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering profile with one or more blocked categories assigned to a source zone that has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue	https://security.paloaltonetworks.com/CVE-2022-0028	O-PAL-PAN--180822/3227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are expected to be released no later than the week of August 15, 2022. This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers and no additional action is required from them. **CVE ID : CVE-2022-0028**		
Affected Version(s): From (including) 8.1 Up to (excluding) 8.1.23-h1					
Uncontrolled Resource Consumption	10-Aug-2022	8.6	A PAN-OS URL filtering policy misconfiguration could allow a network-based	https://security.paloaltonetworks.com/CVE-2022-0028	O-PAL-PAN--180822/3228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto Networks PA-Series (hardware), VM-Series (virtual) and CN-Series (container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering profile with one or more blocked categories assigned to a source zone that has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are expected to be released no later than the week of August 15, 2022. This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers and no additional action is required from them. **CVE ID : CVE-2022-0028**		
Affected Version(s): From (including) 9.0 Up to (excluding) 9.0.16-h3					
Uncontrolled Resource Consumption	10-Aug-2022	8.6	A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto Networks PA-Series (hardware), VM-Series (virtual) and CN-Series	https://security.paloaltonetworks.com/CVE-2022-0028	O-PAL-PAN--180822/3229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering profile with one or more blocked categories assigned to a source zone that has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are expected to be released no later than the week of August 15, 2022.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers and no additional action is required from them. **CVE ID : CVE-2022-0028**		
Affected Version(s): From (including) 9.1 Up to (excluding) 9.1.14-h4					
Uncontrolled Resource Consumption	10-Aug-2022	8.6	A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto Networks PA-Series (hardware), VM-Series (virtual) and CN-Series (container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering profile with one or more blocked categories assigned to a source zone that	https://security.paloaltonetworks.com/CVE-2022-0028	O-PAL-PAN--180822/3230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are expected to be released no later than the week of August 15, 2022. This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers and no additional action is required from them.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-0028		
Vendor: Realtek					
Product: ecos_msdk_firmware					
Affected Version(s): 4.9.4p1					
Improper Input Validation	01-Aug-2022	9.8	In Realtek eCos RSDK 1.5.7p1 and MSDK 4.9.4p1, the SIP ALG function that rewrites SDP data has a stack-based buffer overflow. This allows an attacker to remotely execute code without authentication via a crafted SIP packet that contains malicious SDP data. **CVE ID : CVE-2022-27255**	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2022-27255.pdf	O-REA-ECOS-180822/3231
Product: ecos_rsdk_firmware					
Affected Version(s): 1.5.7p1					
Improper Input Validation	01-Aug-2022	9.8	In Realtek eCos RSDK 1.5.7p1 and MSDK 4.9.4p1, the SIP ALG function that rewrites SDP data has a stack-based buffer overflow. This allows an attacker to remotely execute code without authentication via a crafted SIP packet that contains malicious SDP data. **CVE ID : CVE-2022-27255**	https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2022-27255.pdf	O-REA-ECOS-180822/3232
Vendor: Redhat					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: enterprise_linux					
Affected Version(s): 8.0					
Use After Free	05-Aug-2022	7.8	A flaw was found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the offset to get the page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition. **CVE ID : CVE-2022-1158**	N/A	O-RED-ENTE-180822/3233
Double Free	01-Aug-2022	7.5	A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verification of pkcs7 signatures in gnutls_pkcs7_verify function. **CVE ID : CVE-2022-2509**	https://lists.gnupg.org/pipermail/gnutls-help/2022-July/004746.html	O-RED-ENTE-180822/3234
Affected Version(s): 9.0					
Use After Free	05-Aug-2022	7.8	A flaw was found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the offset to get the	N/A	O-RED-ENTE-180822/3235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition. **CVE ID : CVE-2022-1158**		
Double Free	01-Aug-2022	7.5	A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verification of pkcs7 signatures in gnutls_pkcs7_verify function. **CVE ID : CVE-2022-2509**	https://lists.gnupg.org/pipermail/gnutls-help/2022-July/004746.html	O-RED-ENTE-180822/3236
Product: enterprise_linux_server					
Affected Version(s): 7.9					
N/A	10-Aug-2022	6.5	Linux deployments of StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.2 deployed with a Linux kernel version less than 4.7.0 are susceptible to a vulnerability which could allow a remote	https://security.netapp.com/advisory/NTAP-20220808-0001/	O-RED-ENTE-180822/3237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to view limited metrics information and modify alert email recipients and content. **CVE ID : CVE-2022-23238**		
Vendor: Samsung					
Product: charm_firmware					
Affected Version(s): * Up to (excluding) 1.2.3					
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.5	PendingIntent hijacking vulnerability in releaseAlarm in Charm by Samsung prior to version 1.2.3 allows local attackers to access files without permission via implicit intent. **CVE ID : CVE-2022-36829**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	O-SAM-CHAR-180822/3238
Exposure of Resource to Wrong Sphere	05-Aug-2022	5.5	PendingIntent hijacking vulnerability in cancelAlarmManager in Charm by Samsung prior to version 1.2.3 allows local attackers to access files without permission via implicit intent. **CVE ID : CVE-2022-36830**	https://security.samsungmobile.com/serviceWeb.smsb?year==2022&month=08	O-SAM-CHAR-180822/3239
Missing Authorization	05-Aug-2022	5.5	Unprotected provider vulnerability in	https://security.samsungmobile.com/service	O-SAM-CHAR-180822/3240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Charm by Samsung prior to version 1.2.3 allows attackers to read connection state without permission. **CVE ID : CVE-2022-36836**	Web.smsb?year==2022&month=08	
Vendor: tcl					
Product: linkhub_mesh_wifi_ac1200					
Affected Version(s): ms1g_00_01.00_14					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2022	9.8	An os command injection vulnerability exists in the confsrv ucloud_add_new_node functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to arbitrary command execution. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-21178**	N/A	O-TCL-LINK-180822/3241
N/A	05-Aug-2022	9.8	A denial of service vulnerability exists in the confctl_set_wan_cfg functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to	N/A	O-TCL-LINK-180822/3242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger this vulnerability. **CVE ID : CVE-2022-27178**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-2022	9.8	An os command injection vulnerability exists in the confsrv ucloud_add_node functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to arbitrary command execution. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-22140**	N/A	O-TCL-LINK-180822/3243
Use of Hard-coded Credentials	05-Aug-2022	9.8	A hard-coded password vulnerability exists in the libcommonprod.so prod_change_root_passwd functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. During system startup this functionality is always called, leading to a known root password. An attacker does not have to do anything to trigger this vulnerability.	N/A	O-TCL-LINK-180822/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22144		
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv confctl_set_app_language functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-23103**	N/A	O-TCL-LINK-180822/3245
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv set_port_fwd_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-23399**	N/A	O-TCL-LINK-180822/3246
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists	N/A	O-TCL-LINK-180822/3247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the confsrv set_mf_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.This vulnerability leverages the ethAddr field within the protobuf message to cause a buffer overflow. **CVE ID : CVE-2022-23918**		
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv set_mf_rule functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.This vulnerability leverages the name field within the protobuf message to cause a buffer overflow.	N/A	O-TCL-LINK-180822/3248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23919		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the ap_steer binary. **CVE ID : CVE-2022-24005**	N/A	O-TCL-LINK-180822/3249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within	N/A	O-TCL-LINK-180822/3250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the arpbrocast binary. **CVE ID : CVE-2022-24006**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the cfm binary. **CVE ID : CVE-2022-24007**	N/A	O-TCL-LINK-180822/3251
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the	N/A	O-TCL-LINK-180822/3252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow vulnerability within the confcli binary. **CVE ID : CVE-2022-24008**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the confsrv binary. **CVE ID : CVE-2022-24009**	N/A	O-TCL-LINK-180822/3253
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all	N/A	O-TCL-LINK-180822/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurances of the buffer overflow vulnerability within the cwmpd binary. **CVE ID : CVE-2022-24010**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the device_list binary. **CVE ID : CVE-2022-24011**	N/A	O-TCL-LINK-180822/3255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This	N/A	O-TCL-LINK-180822/3256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability represents all occurances of the buffer overflow vulnerability within the fota binary. **CVE ID : CVE-2022-24012**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the gpio_ctrl binary. **CVE ID : CVE-2022-24013**	N/A	O-TCL-LINK-180822/3257
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this	N/A	O-TCL-LINK-180822/3258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the logserver binary. **CVE ID : CVE-2022-24014**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the log_upload binary. **CVE ID : CVE-2022-24015**	N/A	O-TCL-LINK-180822/3259
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify	N/A	O-TCL-LINK-180822/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the mesh_status_check binary. **CVE ID : CVE-2022-24016**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the miniupnpd binary. **CVE ID : CVE-2022-24017**	N/A	O-TCL-LINK-180822/3261
Buffer Copy without Checking Size of Input ('Classic	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted	N/A	O-TCL-LINK-180822/3262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the multiWAN binary. **CVE ID : CVE-2022-24018**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the netctrl binary. **CVE ID : CVE-2022-24019**	N/A	O-TCL-LINK-180822/3263
Buffer Copy without Checking Size of	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi	N/A	O-TCL-LINK-180822/3264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the network_check binary. **CVE ID : CVE-2022-24020**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the online_process binary. **CVE ID : CVE-2022-24021**	N/A	O-TCL-LINK-180822/3265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the pannn binary. **CVE ID : CVE-2022-24022**	N/A	O-TCL-LINK-180822/3266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the rtk_ate binary.	N/A	O-TCL-LINK-180822/3267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-24024		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the sntp binary. **CVE ID : CVE-2022-24025**	N/A	O-TCL-LINK-180822/3268
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within	N/A	O-TCL-LINK-180822/3269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the telnet_ate_monitor binary. **CVE ID : CVE-2022-24026**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the libcommon.so binary. **CVE ID : CVE-2022-24027**	N/A	O-TCL-LINK-180822/3270
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability	N/A	O-TCL-LINK-180822/3271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			represents all occurances of the buffer overflow vulnerability within the libcommonprod.so binary. **CVE ID : CVE-2022-24028**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the rp-pppoe.so binary. **CVE ID : CVE-2022-24029**	N/A	O-TCL-LINK-180822/3272
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv addTimeGroup functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to a buffer	N/A	O-TCL-LINK-180822/3273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-25996**		
Out-of-bounds Write	05-Aug-2022	9.8	A stack-based buffer overflow vulnerability exists in the confsrv ucloud_set_node_location functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-26009**	N/A	O-TCL-LINK-180822/3274
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-Aug-2022	9.8	A buffer overflow vulnerability exists in the confsrv ucloud_set_node_location functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	N/A	O-TCL-LINK-180822/3275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26342		
N/A	05-Aug-2022	9.8	A denial of service vulnerability exists in the ucloud_del_node functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-26346**	N/A	O-TCL-LINK-180822/3276
Out-of-bounds Write	05-Aug-2022	8.8	A stack-based buffer overflow vulnerability exists in the confers ucloud_add_node_new functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to stack-based buffer overflow. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2022-21201**	N/A	O-TCL-LINK-180822/3277
Buffer Copy without Checking Size of	05-Aug-2022	8.8	A buffer overflow vulnerability exists in the GetValue functionality of TCL LinkHub Mesh Wi-Fi	N/A	O-TCL-LINK-180822/3278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			MS1G_00_01.00_14. A specially-crafted configuration value can lead to a buffer overflow. An attacker can modify a configuration value to trigger this vulnerability.This vulnerability represents all occurances of the buffer overflow vulnerability within the pppd binary. **CVE ID : CVE-2022-24023**		
N/A	05-Aug-2022	7.5	A denial of service vulnerability exists in the confctl_set_master_wlan functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27185**	N/A	O-TCL-LINK-180822/3279
Exposure of Sensitive Information to an Unauthorized Actor	05-Aug-2022	7.5	An information disclosure vulnerability exists in the confctl_get_master_wlan functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14.	N/A	O-TCL-LINK-180822/3280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A specially-crafted network packet can lead to information disclosure. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27630**		
Exposure of Sensitive Information to an Unauthorized Actor	05-Aug-2022	7.5	An information disclosure vulnerability exists in the confctl_get_guest_wlan functionality of TCL LinkHub Mesh Wifi MS1G_00_01.00_14. A specially-crafted network packet can lead to information disclosure. An attacker can send packets to trigger this vulnerability. **CVE ID : CVE-2022-27633**	N/A	O-TCL-LINK-180822/3281
Improper Access Control	05-Aug-2022	7.5	A denial of service vulnerability exists in the confctl_set_guest_wlan functionality of TCL LinkHub Mesh Wi-Fi MS1G_00_01.00_14. A specially-crafted network packet can lead to denial of service. An attacker can send packets to trigger this vulnerability.	N/A	O-TCL-LINK-180822/3282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-27660		
Vendor: tem					
Product: flex-1085_firmware					
Affected Version(s): 1.6.0					
Improper Resource Shutdown or Release	01-Aug-2022	7.5	A vulnerability classified as critical has been found in TEM FLEX-1085 1.6.0. Affected is an unknown function of the file /sistema/flash/reboot. The manipulation leads to denial of service. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2022-2591**	N/A	O-TEM-FLEX-180822/3283
Vendor: totolink					
Product: a3002ru_firmware					
Affected Version(s): 3.0.0-b20220304.1804					
Use of Hard-coded Credentials	10-Aug-2022	9.8	TOTOLINK A3002RU V3.0.0-B20220304.1804 has a hardcoded password for root in /etc/shadow.sample. **CVE ID : CVE-2022-35491**	N/A	O-TOT-A300-180822/3284
Product: a3600r_firmware					
Affected Version(s): 4.1.2cu.5182_b20201102					
Use of Hard-	04-Aug-2022	9.8	Totolink A3600R_Firmware V4.1.2cu.5182_B202	http://www.totolink.cn/home/menu/detail.ht	O-TOT-A360-180822/3285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			01102 contains a hard code password for root in /etc/shadow.sample. **CVE ID : CVE-2022-34993**	ml?menu_listtpl=download&id=63&ids=36image-202206061055 32193	
Vendor: unitree					
Product: go_1_firmware					
Affected Version(s): * Up to (excluding) 0.1.35					
Improper Authentication	05-Aug-2022	6.5	Using off-the-shelf commodity hardware, the Unitree Go 1 robotics platform version H0.1.7 and H0.1.9 (using firmware version 0.1.35) can be powered down by an attacker within normal RF range without authentication. Other versions may be affected, such as the A1. **CVE ID : CVE-2022-2675**	N/A	O-UNI-GO_1-180822/3286
Affected Version(s): * Up to (including) 0.1.35					
Improper Authentication	05-Aug-2022	6.5	Using off-the-shelf commodity hardware, the Unitree Go 1 robotics platform version H0.1.7 and H0.1.9 (using firmware version 0.1.35) can be powered down by an attacker within normal RF range without authentication. Other	N/A	O-UNI-GO_1-180822/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions may be affected, such as the A1. **CVE ID : CVE-2022-2675**		
Vendor: v4l2loopback_project					
Product: v4l2loopback					
Affected Version(s): * Up to (excluding) 0.12.6					
Use of Externally-Controlled Format String	04-Aug-2022	6	Depending on the way the format strings in the card label are crafted it's possible to leak kernel stack memory. There is also the possibility for DoS due to the v4l2loopback kernel module crashing when providing the card label on request (reproduce e.g. with many %s modifiers in a row). **CVE ID : CVE-2022-2652**	https://huntr.dev/bounties/1b055da5-7a9e-4409-99d7-030280d242d5, https://github.com/umlaeute/v4l2loopback/commit/e4cd225557486c420f6a34411f98c575effd43dd	O-V4L-V4L2-180822/3288
Vendor: wavlink					
Product: wn530h4_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection	N/A	O-WAV-WN53-180822/3289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	O-WAV-WN53-180822/3290
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**	N/A	O-WAV-WN53-180822/3291
Improper Neutralization of Special Elements	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3,	N/A	O-WAV-WN53-180822/3292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	O-WAV-WN53-180822/3293
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on	N/A	O-WAV-WN53-180822/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**	N/A	O-WAV-WN53-180822/3295
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**	N/A	O-WAV-WN53-180822/3296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	O-WAV-WN53-180822/3297
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**	N/A	O-WAV-WN53-180822/3298
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml.	N/A	O-WAV-WN53-180822/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35534		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	O-WAV-WN53-180822/3300
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	O-WAV-WN53-180822/3301
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname,	N/A	O-WAV-WN53-180822/3302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**	N/A	O-WAV-WN53-180822/3303
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command	N/A	O-WAV-WN53-180822/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**		
Product: wn531p3_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**	N/A	O-WAV-WN53-180822/3305
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	O-WAV-WN53-180822/3306
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	O-WAV-WN53-180822/3307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**	N/A	O-WAV-WN53-180822/3308
Improper Neutralization of Special Elements used in a Command	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on	N/A	O-WAV-WN53-180822/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**	N/A	O-WAV-WN53-180822/3310
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command	N/A	O-WAV-WN53-180822/3311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**	N/A	O-WAV-WN53-180822/3312
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	O-WAV-WN53-180822/3313
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command	N/A	O-WAV-WN53-180822/3314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injection in page /qos.shtml. **CVE ID : CVE-2022-35533**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**	N/A	O-WAV-WN53-180822/3315
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	O-WAV-WN53-180822/3316
Improper Neutralization of Special Elements used in a	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi	N/A	O-WAV-WN53-180822/3317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**	N/A	O-WAV-WN53-180822/3318
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml.	N/A	O-WAV-WN53-180822/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35538		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**	N/A	O-WAV-WN53-180822/3320
Product: wn533a8_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**	N/A	O-WAV-WN53-180822/3321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	O-WAV-WN53-180822/3322
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**	N/A	O-WAV-WN53-180822/3323
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagement	N/A	O-WAV-WN53-180822/3324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			Enabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	O-WAV-WN53-180822/3325
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection	N/A	O-WAV-WN53-180822/3326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**	N/A	O-WAV-WN53-180822/3327
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**	N/A	O-WAV-WN53-180822/3328
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	O-WAV-WN53-180822/3329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**	N/A	O-WAV-WN53-180822/3330
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**	N/A	O-WAV-WN53-180822/3331
Improper Neutralizat	10-Aug-2022	9.8	WAVLINK WN572HP3,	N/A	O-WAV-WN53-180822/3332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	O-WAV-WN53-180822/3333
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml.	N/A	O-WAV-WN53-180822/3334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35537		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**	N/A	O-WAV-WN53-180822/3335
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml.	N/A	O-WAV-WN53-180822/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35517		
Product: wn535g3_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**	N/A	O-WAV-WN53-180822/3337
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**	N/A	O-WAV-WN53-180822/3338
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf,	N/A	O-WAV-WN53-180822/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**	N/A	O-WAV-WN53-180822/3340
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway,	N/A	O-WAV-WN53-180822/3341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35523**	N/A	O-WAV-WN53-180822/3342
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml.	N/A	O-WAV-WN53-180822/3343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35524		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**	N/A	O-WAV-WN53-180822/3344
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**	N/A	O-WAV-WN53-180822/3345
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml.	N/A	O-WAV-WN53-180822/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35533		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**	N/A	O-WAV-WN53-180822/3347
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**	N/A	O-WAV-WN53-180822/3348
Improper Neutralization of Special Elements used in a Command ('Comman	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters:	N/A	O-WAV-WN53-180822/3349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**	N/A	O-WAV-WN53-180822/3350
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**	N/A	O-WAV-WN53-180822/3351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**	N/A	O-WAV-WN53-180822/3352
Product: wn572hp3_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml. **CVE ID : CVE-2022-35518**	N/A	O-WAV-WN57-180822/3353
Improper Neutralizat	10-Aug-2022	9.8	WAVLINK WN572HP3,	N/A	O-WAV-WN57-180822/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml. **CVE ID : CVE-2022-35519**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35520**	N/A	O-WAV-WN57-180822/3355
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnable	N/A	O-WAV-WN57-180822/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			d, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml. **CVE ID : CVE-2022-35521**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml. **CVE ID : CVE-2022-35522**	N/A	O-WAV-WN57-180822/3357
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml.	N/A	O-WAV-WN57-180822/3358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-35523		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml. **CVE ID : CVE-2022-35524**	N/A	O-WAV-WN57-180822/3359
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml. **CVE ID : CVE-2022-35525**	N/A	O-WAV-WN57-180822/3360
Improper Neutralization of Special Elements used in a	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi	N/A	O-WAV-WN57-180822/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			has no filtering on parameter key, which leads to command injection in page /login.shtml. **CVE ID : CVE-2022-35526**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35533**	N/A	O-WAV-WN57-180822/3362
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml. **CVE ID : CVE-2022-35534**	N/A	O-WAV-WN57-180822/3363
Improper Neutralization of Special	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4,	N/A	O-WAV-WN57-180822/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35535**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml. **CVE ID : CVE-2022-35536**	N/A	O-WAV-WN57-180822/3365
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35537**	N/A	O-WAV-WN57-180822/3366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	9.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml. **CVE ID : CVE-2022-35538**	N/A	O-WAV-WN57-180822/3367
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-Aug-2022	8.8	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml. **CVE ID : CVE-2022-35517**	N/A	O-WAV-WN57-180822/3368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: yoctoproject					
Product: yocto					
Affected Version(s): 3.1					
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3369
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3370
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds	https://corp.mediatek.com/product-security-	O-YOC-YOCT-180822/3371

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: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	bulletin/August-2022	
Access of Resource Using Incompatible Type ('Type Confusion')	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3372
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due 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/August-2022	O-YOC-YOCT-180822/3373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435; Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3374
Affected Version(s): 3.3					
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032521; Issue ID: ALPS07032521. **CVE ID : CVE-2022-26430**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032553; Issue ID: ALPS07032553. **CVE ID : CVE-2022-26431**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3376
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07032542; Issue ID: ALPS07032542. **CVE ID : CVE-2022-26432**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3377
Access of Resource Using Incompatible Type	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138400; Issue ID: ALPS07138400. **CVE ID : CVE-2022-26433**		
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138450; Issue ID: ALPS07138450. **CVE ID : CVE-2022-26434**	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3379
Out-of-bounds Write	01-Aug-2022	6.7	In mailbox, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07138435;	https://corp.mediatek.com/product-security-bulletin/August-2022	O-YOC-YOCT-180822/3380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Issue ID: ALPS07138435. **CVE ID : CVE-2022-26435**		