National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 – 31 Jul 2023 Vol. 10 No. 14

Table of Content

Vendor	Product	Page Number
HP	color_laserjet_pro_4201-4203_4ra88f_firmware	699
	color_laserjet_pro_4201-4203_4ra89a_firmware	700
	color_laserjet_pro_4201-4203_5hh48a_firmware	700
	color_laserjet_pro_4201-4203_5hh51a_firmware	700
	color_laserjet_pro_4201-4203_5hh52a_firmware	701
	color_laserjet_pro_4201-4203_5hh53a_firmware	701
	color_laserjet_pro_4201-4203_5hh59a_firmware	701
	color_laserjet_pro_mfp_4301-4303_4ra80f_firmware	702
	color_laserjet_pro_mfp_4301-4303_4ra81f_firmware	702
	color_laserjet_pro_mfp_4301-4303_4ra82f_firmware	702
	color_laserjet_pro_mfp_4301-4303_4ra83f_firmware	703
	color_laserjet_pro_mfp_4301-4303_4ra84f_firmware	703
	color_laserjet_pro_mfp_4301-4303_5hh64f_firmware	704
	color_laserjet_pro_mfp_4301-4303_5hh65a_firmware	704
	color_laserjet_pro_mfp_4301-4303_5hh66a_firmware	704
	color_laserjet_pro_mfp_4301-4303_5hh67a_firmware	705
	color_laserjet_pro_mfp_4301-4303_5hh72a_firmware	705
	color_laserjet_pro_mfp_4301-4303_5hh73a_firmware	705
	hp-ux	706

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: activeitzone					
Product: active_super_shop					
Affected Version(s): 2.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	5.4	A vulnerability, which was classified as problematic, has been found in ActiveITzone Active Super Shop CMS 2.5. This issue affects some unknown processing of the component Manage Details Page. The manipulation of the argument name/phone/address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235055. **CVE ID : CVE-2023-3788**	N/A	A-ACT-ACTI-020823/1
Vendor: Admidio					
Product: admidio					
Affected Version(s): * Up to (excluding) 4.2.10					
Unrestricted Upload of File with Dangerous Type	16-Jul-2023	7.2	Unrestricted Upload of File with Dangerous Type in GitHub repository admidio/admidio prior to 4.2.10.	https://huntr.dev/bounties/be6616eb-384d-40d6-b1fd-0ec9e4973f12,	A-ADM-ADMI-020823/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3692	https://github.com/admidio/admidio/commit/d66585d14b1160712a8a9bfaf9769dd3da0e9a83	
Vendor: Adobe					
Product: coldfusion					
Affected Version(s): 2018					
Deserialization of Untrusted Data	20-Jul-2023	9.8	Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38203**	https://helpx.adobe.com/security/products/coldfusion/apsb23-41.html	A-ADO-COLD-020823/3
Affected Version(s): 2021					
Deserialization of Untrusted Data	20-Jul-2023	9.8	Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this	https://helpx.adobe.com/security/products/coldfusion/apsb23-41.html	A-ADO-COLD-020823/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID : CVE-2023-38203**		
Affected Version(s): 2023					
Deserialization of Untrusted Data	20-Jul-2023	9.8	Adobe ColdFusion versions 2018u17 (and earlier), 2021u7 (and earlier) and 2023u1 (and earlier) are affected by a Deserialization of Untrusted Data vulnerability that could result in Arbitrary code execution. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2023-38203**	https://helpx.adobe.com/security/products/coldfusion/apsb23-41.html	A-ADO-COLD-020823/5
Vendor: advancedplugins					
Product: ultimateimagetool					
Affected Version(s): * Up to (excluding) 2.1.03					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jul-2023	7.5	In the module "Image: WebP, Compress, Zoom, Lazy load, Alt & More" (ultimateimagetool) in versions up to 2.1.02 from Advanced Plugins for PrestaShop, a guest can download personal informations without restriction by performing a path traversal attack. **CVE ID : CVE-2023-30200**	https://security.friendsofpresta.org/modules/2023/07/20/ultimateimagetool.html	A-ADV-ULTI-020823/6

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: agentejo					
Product: cockpit					
Affected Version(s): * Up to (including) 2.5.2					
Cross-Site Request Forgery (CSRF)	20-Jul-2023	8.8	A Cross-Site Request Forgery (CSRF) in the Admin portal of Cockpit CMS v2.5.2 allows attackers to execute arbitrary Administrator commands. **CVE ID : CVE-2023-37650**	N/A	A-AGE-COCK-020823/7
N/A	20-Jul-2023	7.5	Incorrect access control in the component /models/Content of Cockpit CMS v2.5.2 allows unauthorized attackers to access sensitive data. **CVE ID : CVE-2023-37649**	N/A	A-AGE-COCK-020823/8
Vendor: aiohttp_project					
Product: aiohttp					
Affected Version(s): * Up to (including) 3.8.4					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	19-Jul-2023	7.5	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. aiohttp v3.8.4 and earlier are bundled with llhttp v6.0.6. Vulnerable code is used by aiohttp for its HTTP request parser when available which is the default case when installing from a wheel. This	https://github.com/aio-libs/aiohttp/security/advisories/GHSA-45c4-8wx5-qw6w, https://github.com/aio-libs/aiohttp/commit/9337fb3f2ab2b5f38d7e98a1	A-AIO-AIOH-020823/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects users of aiohttp as an HTTP server (ie `aiohttp.Application`), you are not affected by this vulnerability if you are using aiohttp as an HTTP client library (ie `aiohttp.ClientSession`). Sending a crafted HTTP request will cause the server to misinterpret one of the HTTP header values leading to HTTP request smuggling. This issue has been addressed in version 3.8.5. Users are advised to upgrade. Users unable to upgrade can reinstall aiohttp using `AIOHTTP_NO_EXTENSIONS=1` as an environment variable to disable the llhttp HTTP request parser implementation. The pure Python implementation isn't vulnerable. **CVE ID : CVE-2023-37276**	94bde6f7e3d16c40	
Vendor: Alkacon					
Product: opencms					
Affected Version(s): 15.0.0					
Improper Neutralization of Input	20-Jul-2023	6.1	An arbitrary file upload vulnerability in the component /workplace#!explorer	N/A	A-ALK-OPEN-020823/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			of Alkacon OpenCMS v15.0 allows attackers to execute arbitrary code via uploading a crafted PNG file. **CVE ID : CVE-2023-37602**		
Vendor: an_gradebook_project					
Product: an_gradebook					
Affected Version(s): * Up to (including) 5.0.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2023	8.8	The AN_GradeBook WordPress plugin through 5.0.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as subscriber **CVE ID : CVE-2023-2636**	N/A	A-AN_-AN_G-020823/11
Vendor: Apache					
Product: eventmesh					
Affected Version(s): From (including) 1.7.0 Up to (including) 1.8.0					
Deserialization of Untrusted Data	17-Jul-2023	9.8	CWE-502 Deserialization of Untrusted Data at the rabbitmq-connector plugin module in Apache EventMesh (incubating) V1.7.0\V1.8.0 on windows\linux\mac os e.g. platforms allows attackers to send controlled message and	N/A	A-APA-EVEN-020823/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execute via rabbitmq messages. Users can use the code under the master branch in project repo to fix this issue, we will release the new version as soon as possible. **CVE ID : CVE-2023-26512**		
Product: shardingsphere					
Affected Version(s): * Up to (excluding) 5.4.0					
Deserialization of Untrusted Data	19-Jul-2023	8.8	Deserialization of Untrusted Data vulnerability in Apache ShardingSphere-Agent, which allows attackers to execute arbitrary code by constructing a special YAML configuration file. The attacker needs to have permission to modify the ShardingSphere Agent YAML configuration file on the target machine, and the target machine can access the URL with the arbitrary code JAR. An attacker can use SnakeYAML to deserialize java.net.URLClassLoader and make it load a JAR from a specified URL, and then deserialize	N/A	A-APA-SHAR-020823/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			javax.script.ScriptEngineManager to load code using that ClassLoader. When the ShardingSphere JVM process starts and uses the ShardingSphere-Agent, the arbitrary code specified by the attacker will be executed during the deserialization of the YAML configuration file by the Agent. This issue affects ShardingSphere-Agent: through 5.3.2. This vulnerability is fixed in Apache ShardingSphere 5.4.0. **CVE ID : CVE-2023-28754**		
Vendor: artbees					
Product: jupiter_x_core					
Affected Version(s): * Up to (including) 2.5.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jul-2023	7.5	The Jupiter X Core plugin for WordPress is vulnerable to arbitrary file downloads in versions up to, and including, 2.5.0. This makes it possible for unauthenticated attackers to download the contents of arbitrary files on the server, which can contain sensitive information. The requires the premium	N/A	A-ART-JUPI-020823/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version of the plugin to be activated. **CVE ID : CVE-2023-3813**		
Vendor: assemblysoftware					
Product: trialworks					
Affected Version(s): 11.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	6.1	A cross-site scripting (XSS) vulnerability in Assembly Software Trialworks v11.4 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the asset src parameter. **CVE ID : CVE-2023-37613**	N/A	A-ASS-TRIA-020823/15
Vendor: Atlassian					
Product: bamboo_data_center					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 9.2.3					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	8.8	This High severity Injection and RCE (Remote Code Execution) vulnerability known as CVE-2023-22506 was introduced in version 8.0.0 of Bamboo Data Center. This Injection and RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.5, allows an authenticated attacker to	https://jira.atlassian.com/browse/BAM-22400	A-ATL-BAMB-020823/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modify the actions taken by a system call and execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to latest version. If you're unable to upgrade to latest, upgrade to one of these fixed versions: 9.2.3 and 9.3.1. See the release notes ([https://confluence.atlassian.com/bamboorelease s/bamboo-release-notes-1189793869.html|https://confluence.atlassian.com/bamboorelease s/bamboo-release-notes-1189793869.html]). You can download the latest version of Bamboo Data Center and Bamboo Server from the download center ([https://www.atlassian.com/software/bamboo/download-archives|https://www.atlassian.com/software/bamboo/download-archives]).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability was reported via our Penetration Testing program. **CVE ID : CVE-2023-22506**		
Product: bamboo_server					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 9.2.3					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	8.8	This High severity Injection and RCE (Remote Code Execution) vulnerability known as CVE-2023-22506 was introduced in version 8.0.0 of Bamboo Data Center. This Injection and RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.5, allows an authenticated attacker to modify the actions taken by a system call and execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to latest version. If you're unable to upgrade to latest, upgrade to one of these fixed versions:	https://jira.atlassian.com/browse/BAM-22400	A-ATL-BAMB-020823/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.2.3 and 9.3.1. See the release notes ([https://confluence.atlassian.com/bamboorelease s/bamboo-release-notes-1189793869.html|https://confluence.atlassian.com/bamboorelease s/bamboo-release-notes-1189793869.html]). You can download the latest version of Bamboo Data Center and Bamboo Server from the download center ([https://www.atlassian.com/software/bamboo/download-archives|https://www.atlassian.com/software/bamboo/download-archives]). This vulnerability was reported via our Penetration Testing program. **CVE ID : CVE-2023-22506**		
Product: confluence_data_center					
Affected Version(s): From (including) 6.1.0 Up to (excluding) 7.13.20					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22508 was introduced in version 6.1.0 of Confluence Data Center & Server. This	https://jira.atlassian.com/browse/CONFSERVER-88221	A-ATL-CONF-020823/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to avoid this bug using the following options: * Upgrade to a Confluence feature release greater than or equal to 8.2.0 (ie: 8.2, 8.2, 8.4, etc...) * Upgrade to a Confluence 7.19 LTS bugfix release greater than or equal to 7.19.8 (ie: 7.19.8, 7.19.9, 7.19.10, 7.19.11, etc...) * Upgrade to a Confluence 7.13 LTS bugfix release greater than or equal to 7.13.20 (Release available early August) See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Data Center		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			& Server from the download center (https://www.atlassian.com/software/confluence/download-archives). If you are unable to upgrade your instance please use the following guide to workaround the issue https://confluence.atlassian.com/confkb/how-to-disable-the-jmx-network-port-for-cve-2023-22508-1267761550.html This vulnerability was discovered by a private user and reported via our Bug Bounty program. **CVE ID : CVE-2023-22508**		
Affected Version(s): From (including) 7.14.0 Up to (excluding) 7.19.8					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22508 was introduced in version 6.1.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to	https://jira.atlassian.com/browse/CONFSERVER-88221	A-ATL-CONF-020823/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to avoid this bug using the following options: * Upgrade to a Confluence feature release greater than or equal to 8.2.0 (ie: 8.2, 8.2, 8.4, etc...) * Upgrade to a Confluence 7.19 LTS bugfix release greater than or equal to 7.19.8 (ie: 7.19.8, 7.19.9, 7.19.10, 7.19.11, etc...) * Upgrade to a Confluence 7.13 LTS bugfix release greater than or equal to 7.13.20 (Release available early August) See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Data Center & Server from the download center (https://www.atlassian.com/software/confluence/download-archives). If you are unable to upgrade your instance please use the following		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			guide to workaround the issue https://confluence.atlassian.com/confkb/how-to-disable-the-jmx-network-port-for-cve-2023-22508-1267761550.html This vulnerability was discovered by a private user and reported via our Bug Bounty program. **CVE ID : CVE-2023-22508**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.2.0					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22508 was introduced in version 6.1.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to avoid this bug using the	https://jira.atlassian.com/browse/CONFSERVER-88221	A-ATL-CONF-020823/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			following options: * Upgrade to a Confluence feature release greater than or equal to 8.2.0 (ie: 8.2, 8.2, 8.4, etc...) * Upgrade to a Confluence 7.19 LTS bugfix release greater than or equal to 7.19.8 (ie: 7.19.8, 7.19.9, 7.19.10, 7.19.11, etc...) * Upgrade to a Confluence 7.13 LTS bugfix release greater than or equal to 7.13.20 (Release available early August) See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Data Center & Server from the download center (https://www.atlassian.com/software/confluence/download-archives). If you are unable to upgrade your instance please use the following guide to workaround the issue https://confluence.atlassian.com/confkb/how-to-disable-the-jmx-network-port-for-cve-2023-22508-1267761550.html This vulnerability was		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discovered by a private user and reported via our Bug Bounty program. **CVE ID : CVE-2023-22508**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.3.2					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22505 was introduced in version 8.0.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to latest version. If you're unable to upgrade to latest, upgrade to one of these fixed versions: 8.3.2, 8.4.0. See the release notes ([https://confluence.a	https://jira.atlassian.com/browse/CONFSERVER-88265	A-ATL-CONF-020823/21

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tlassian.com/doc/confluence-release-notes-327.html).|https://confluence.atlassian.com/doc/confluence-release-notes-327.html).] You can download the latest version of Confluence Data Center & Server from the download center ([https://www.atlassian.com/software/confluence/download-archives).|https://www.atlassian.com/software/confluence/download-archives).] This vulnerability was discovered by a private user and reported via our Bug Bounty program. **CVE ID : CVE-2023-22505**		
Product: confluence_server					
Affected Version(s): From (including) 6.1.0 Up to (excluding) 7.13.20					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22508 was introduced in version 6.1.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5,	https://jira.atlassian.com/browse/CONFSERVER-88221	A-ATL-CONF-020823/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to avoid this bug using the following options: * Upgrade to a Confluence feature release greater than or equal to 8.2.0 (ie: 8.2, 8.2, 8.4, etc...) * Upgrade to a Confluence 7.19 LTS bugfix release greater than or equal to 7.19.8 (ie: 7.19.8, 7.19.9, 7.19.10, 7.19.11, etc...) * Upgrade to a Confluence 7.13 LTS bugfix release greater than or equal to 7.13.20 (Release available early August) See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Data Center & Server from the download center (https://www.atlassian.com/software/confl		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uence/download-archives). If you are unable to upgrade your instance please use the following guide to workaround the issue https://confluence.atlassian.com/confkb/how-to-disable-the-jmx-network-port-for-cve-2023-22508-1267761550.html This vulnerability was discovered by a private user and reported via our Bug Bounty program. **CVE ID : CVE-2023-22508**		
Affected Version(s): From (including) 7.14.0 Up to (excluding) 7.19.8					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22508 was introduced in version 6.1.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no	https://jira.atlassian.com/browse/CONFSERVER-88221	A-ATL-CONF-020823/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user interaction. Atlassian recommends that you upgrade your instance to avoid this bug using the following options: * Upgrade to a Confluence feature release greater than or equal to 8.2.0 (ie: 8.2, 8.2, 8.4, etc...) * Upgrade to a Confluence 7.19 LTS bugfix release greater than or equal to 7.19.8 (ie: 7.19.8, 7.19.9, 7.19.10, 7.19.11, etc...) * Upgrade to a Confluence 7.13 LTS bugfix release greater than or equal to 7.13.20 (Release available early August) See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Data Center & Server from the download center (https://www.atlassian.com/software/confluence/download-archives). If you are unable to upgrade your instance please use the following guide to workaround the issue https://confluence.atlassian.com/confkb/ho		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			w-to-disable-the-jmx-network-port-for-cve-2023-22508-1267761550.html This vulnerability was discovered by a private user and reported via our Bug Bounty program. **CVE ID : CVE-2023-22508**		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.2.0					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22508 was introduced in version 6.1.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to avoid this bug using the following options: * Upgrade to a Confluence feature release greater than or	https://jira.atlassian.com/browse/CONFSERVER-88221	A-ATL-CONF-020823/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			equal to 8.2.0 (ie: 8.2, 8.2, 8.4, etc...) * Upgrade to a Confluence 7.19 LTS bugfix release greater than or equal to 7.19.8 (ie: 7.19.8, 7.19.9, 7.19.10, 7.19.11, etc...) * Upgrade to a Confluence 7.13 LTS bugfix release greater than or equal to 7.13.20 (Release available early August) See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Data Center & Server from the download center (https://www.atlassian.com/software/confluence/download-archives). If you are unable to upgrade your instance please use the following guide to workaround the issue https://confluence.atlassian.com/confkb/how-to-disable-the-jmx-network-port-for-cve-2023-22508-1267761550.html This vulnerability was discovered by a private user and reported via our Bug Bounty program.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22508		
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.3.2					
N/A	18-Jul-2023	8.8	This High severity RCE (Remote Code Execution) vulnerability known as CVE-2023-22505 was introduced in version 8.0.0 of Confluence Data Center & Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction. Atlassian recommends that you upgrade your instance to latest version. If you're unable to upgrade to latest, upgrade to one of these fixed versions: 8.3.2, 8.4.0. See the release notes ([https://confluence.atlassian.com/doc/confluence-release-notes-327.html).|https://confluence.atlassian.com/doc/confluence-release-notes-327.html).] You can	https://jira.atlassian.com/browse/CONFSERVER-88265	A-ATL-CONF-020823/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download the latest version of Confluence Data Center & Server from the download center ([https://www.atlassian.com/software/confluence/download-archives).|https://www.atlassian.com/software/confluence/download-archives).] This vulnerability was discovered by a private user and reported via our Bug Bounty program. **CVE ID : CVE-2023-22505**		
Vendor: autochat					
Product: automatic_conversation					
Affected Version(s): * Up to (including) 1.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	The Autochat Automatic Conversation WordPress plugin through 1.1.7 does not sanitise and escape user input before outputting it back on the page, leading to a cross-site Scripting attack. **CVE ID : CVE-2023-3041**	N/A	A-AUT-AUTO-020823/26
Vendor: auto_location_for_wp_job_manager_via_google_project					
Product: auto_location_for_wp_job_manager_via_google					
Affected Version(s): * Up to (excluding) 1.1					
Improper Neutralizat	24-Jul-2023	4.8	The Auto Location for WP Job Manager via	N/A	A-AUT-AUTO-020823/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Google WordPress plugin before 1.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-3344**		
Vendor: Avaya					
Product: aura_device_services					
Affected Version(s): * Up to (including) 8.1.4.0					
Unrestricted Upload of File with Dangerous Type	19-Jul-2023	9.8	An OS command injection vulnerability was found in the Avaya Aura Device Services Web application which could allow remote code execution as the Web server user via a malicious uploaded file. This issue affects Avaya Aura Device Services version 8.1.4.0 and earlier. **CVE ID : CVE-2023-3722**	N/A	A-AVA-AURA-020823/28
Product: call_management_system					
Affected Version(s): * Up to (excluding) 20.0.0.0					
Improper Neutralization of	18-Jul-2023	6.8	A CSV injection vulnerability was found in the Avaya	https://download.avaya.com/css/pu	A-AVA-CALL-020823/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Formula Elements in a CSV File			Call Management System (CMS) Supervisor web application which allows a user with administrative privileges to input crafted data which, when exported to a CSV file, may attempt arbitrary command execution on the system used to open the file by a spreadsheet software such as Microsoft Excel. **CVE ID : CVE-2023-3527**	blic/documents/101086364	
Vendor: avro_project					
Product: avro					
Affected Version(s): * Up to (excluding) 2.13.0					
Uncontrolled Resource Consumption	17-Jul-2023	7.5	Hamba avro is a go lang encoder/decoder implementation of the avro codec specification. In affected versions a well-crafted string passed to avro's `github.com/hamba/avro/v2.Unmarshal()` can throw a `fatal error: runtime: out of memory` which is unrecoverable and can cause denial of service of the consumer of avro. The root cause of the issue is that avro uses part of the input to `Unmarshal()` to	https://github.com/hamba/avro/commit/b4a402f41cf44b6094b5131286830ba9bb1eb290, https://github.com/hamba/avro/security/advisories/GHSA-9x44-9pgq-cf45	A-AVR-AVRO-020823/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			determine the size when creating a new slice and hence an attacker may consume arbitrary amounts of memory which in turn may cause the application to crash. This issue has been addressed in commit `b4a402f4` which has been included in release version `2.13.0`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37475**		
Vendor: awplife					
Product: album_gallery					
Affected Version(s): * Up to (excluding) 1.5.0					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in A WP Life Album Gallery – WordPress Gallery plugin <= 1.4.9 versions. **CVE ID : CVE-2023-23646**	N/A	A-AWP-ALBU-020823/31
Vendor: basixonline					
Product: nex-forms					
Affected Version(s): * Up to (excluding) 8.4.4					
Improper Neutralization of Input During Web Page	17-Jul-2023	5.4	The NEX-Forms WordPress plugin before 8.4.4 does not escape its form name, which could lead to Stored Cross-Site	N/A	A-BAS-NEX--020823/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Scripting issues. By default only SuperAdmins (in multisite) / admins (in single site) can create forms, however there is a settings allowing them to give lower roles access to such feature. **CVE ID : CVE-2023-0439**		
Vendor: beauty_salon_management_system_project					
Product: beauty_salon_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2023	9.8	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file add-product.php. The manipulation of the argument category 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-234252. **CVE ID : CVE-2023-3695**	N/A	A-BEA-BEAU-020823/33
Improper Neutralization of Special Elements	21-Jul-2023	8.8	A vulnerability has been found in Campcodes Beauty Salon Management System 1.0 and	N/A	A-BEA-BEAU-020823/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			classified as critical. Affected by this vulnerability is an unknown functionality of the file edit_product.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235075. **CVE ID : CVE-2023-3807**		
Vendor: biltay					
Product: scienta					
Affected Version(s): * Up to (excluding) 20230630.1953					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Biltay Technology Scienta allows SQL Injection.This issue affects Scienta: before 20230630.1953. **CVE ID : CVE-2023-3046**	N/A	A-BIL-SCIE-020823/35
Vendor: booking_calendar_project					
Product: booking_calendar					
Affected Version(s): * Up to (including) 1.2.40					
Improper Neutralization of	18-Jul-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in	N/A	A-BOO-BOOK-020823/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			CodePeople Booking Calendar Contact Form plugin <= 1.2.40 versions. **CVE ID : CVE-2023-36384**		
Vendor: bugfinder					
Product: chaincity					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jul-2023	9.8	A vulnerability classified as critical was found in Bug Finder ChainCity Real Estate Investment Platform 1.0. Affected by this vulnerability is an unknown functionality of the file /property of the component GET Parameter Handler. The manipulation of the argument name leads to sql injection. The associated identifier of this vulnerability is VDB-235063. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3795**	N/A	A-BUG-CHAI-020823/37
Improper Neutralization of Input During Web Page Generation	20-Jul-2023	6.1	A vulnerability classified as problematic has been found in Bug Finder ChainCity Real Estate Investment Platform 1.0. Affected is an unknown function of	N/A	A-BUG-CHAI-020823/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the file /chaincity/user/ticket /create of the component New Ticket Handler. The manipulation of the argument subject leads to cross site scripting. It is possible to launch the attack remotely. VDB-235062 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3794**		
Product: ex-rate					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability was found in Bug Finder EX-RATE 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235160. NOTE: The	N/A	A-BUG-EX-R-020823/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3834**		
Product: finounce					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	A vulnerability was found in Bug Finder Finounce 1.0 and classified as problematic. This issue affects some unknown processing of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-235157 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3831**	N/A	A-BUG-FINO-020823/40
Product: foody_friend					
Affected Version(s): 1.0					
Unrestricted Upload of File with	20-Jul-2023	8.8	A vulnerability, which was classified as problematic, has been found in Bug Finder	N/A	A-BUG-FOOD-020823/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Foody Friend 1.0. Affected by this issue is some unknown functionality of the file /user/profile of the component Profile Picture Handler. The manipulation of the argument profile_picture leads to unrestricted upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-235064. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3796**		
Product: icogenie					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability was found in Bug Finder ICOGenie 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /user/ticket/create of the component Support Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack can be initiated remotely. VDB-	N/A	A-BUG-ICOG-020823/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			235150 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3829**		
Product: listplace_directory_listing_platform					
Affected Version(s): 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability was found in Bug Finder Listplace Directory Listing Platform 3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /listplace/user/ticket/create of the component HTTP POST Request Handler. The manipulation of the argument message leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235148. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3827**	N/A	A-BUG-LIST-020823/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability was found in Bug Finder Listplace Directory Listing Platform 3.0. It has been classified as problematic. This affects an unknown part of the file /listplace/user/coverPhotoUpdate of the component Photo Handler. The manipulation of the argument user_cover_photo leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235149 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3828**	N/A	A-BUG-LIST-020823/44
Product: minestack					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability classified as problematic has been found in Bug Finder MineStack 1.0. This affects an unknown part of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message	N/A	A-BUG-MINE-020823/45

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235161 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3835**		
Product: montage					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability was found in Bug Finder Montage 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /user/ticket/create of the component Ticket Handler. The manipulation of the argument message leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235159. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-BUG-MONT-020823/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3833		
Product: sass_biller					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability was found in Bug Finder SASS BILLER 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /company/store. The manipulation of the argument name leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-235151. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3830**	N/A	A-BUG-SASS-020823/47
Product: wedding_wonders					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	6.1	A vulnerability was found in Bug Finder Wedding Wonders 1.0. It has been classified as problematic. Affected is an unknown function of the file /user/ticket/create of the component Ticket Handler. The manipulation of the	N/A	A-BUG-WEDD-020823/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument message leads to cross site scripting. It is possible to launch the attack remotely. VDB-235158 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3832**		
Vendor: bylancer					
Product: quickai_openai					
Affected Version(s): 3.8.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2023	9.8	A vulnerability was found in Bylancer QuickAI OpenAI 3.8.1. It has been declared as critical. This vulnerability affects unknown code of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-234232. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3686**	N/A	A-BYL-QUIC-020823/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: quickjob					
Affected Version(s): 6.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2023	9.8	A vulnerability classified as critical has been found in Bylancer QuickJob 6.1. Affected is an unknown function of the component GET Parameter Handler. The manipulation of the argument keywords/gender leads to sql injection. It is possible to launch the attack remotely. VDB-234234 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3688**	N/A	A-BYL-QUIC-020823/50
Product: quickorder					
Affected Version(s): 6.3.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2023	9.8	A vulnerability, which was classified as critical, has been found in Bylancer QuickOrder 6.3.7. Affected by this issue is some unknown functionality of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The	N/A	A-BYL-QUIC-020823/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack may be launched remotely. The identifier of this vulnerability is VDB-234236. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3690**		
Product: quickqr					
Affected Version(s): 6.3.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2023	9.8	A vulnerability classified as critical was found in Bylancer QuickQR 6.3.7. Affected by this vulnerability is an unknown functionality of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-234235. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3689**	N/A	A-BYL-QUIC-020823/52
Product: quickvcard					
Affected Version(s): 2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2023	9.8	A vulnerability was found in Bylancer QuickVCard 2.1. It has been rated as critical. This issue affects some unknown processing of the file /blog of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The attack may be initiated remotely. The identifier VDB-234233 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3687**	N/A	A-BYL-QUIC-020823/53
Vendor: campcodes					
Product: beauty_salon_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jul-2023	7.5	A vulnerability classified as critical has been found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/edit_category.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely.	N/A	A-CAM-BEAU-020823/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The identifier VDB-235233 was assigned to this vulnerability. **CVE ID : CVE-2023-3871**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jul-2023	7.5	A vulnerability classified as critical was found in Campcodes Beauty Salon Management System 1.0. This vulnerability affects unknown code of the file /admin/edit-services.php. The manipulation of the argument editid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235234 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3872**	N/A	A-CAM-BEAU-020823/55
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	7.5	A vulnerability, which was classified as critical, has been found in Campcodes Beauty Salon Management System 1.0. This issue affects some unknown processing of the file /admin/index.php. The manipulation of the argument username leads to sql	N/A	A-CAM-BEAU-020823/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-235235. **CVE ID : CVE-2023-3873**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	7.5	A vulnerability, which was classified as critical, was found in Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file /admin/admin-profile.php. The manipulation of the argument adminname 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-235236. **CVE ID : CVE-2023-3874**	N/A	A-CAM-BEAU-020823/57
Improper Neutralization of Special Elements used in an SQL Command	25-Jul-2023	7.5	A vulnerability was found in Campcodes Beauty Salon Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file	N/A	A-CAM-BEAU-020823/58

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			/admin/search-appointment.php. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-235238 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3876**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	7.5	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/add-services.php. The manipulation of the argument cost 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-235239. **CVE ID : CVE-2023-3877**	N/A	A-CAM-BEAU-020823/59
Improper Neutralization of Special Elements	25-Jul-2023	7.5	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been	N/A	A-CAM-BEAU-020823/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			declared as critical. This vulnerability affects unknown code of the file /admin/about-us.php. The manipulation of the argument pagedes leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235240. **CVE ID : CVE-2023-3878**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	7.5	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/del_category.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235241 was assigned to this vulnerability. **CVE ID : CVE-2023-3879**	N/A	A-CAM-BEAU-020823/61
Improper Neutralization of	25-Jul-2023	7.5	A vulnerability classified as critical has been found in	N/A	A-CAM-BEAU-020823/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			Campcodes Beauty Salon Management System 1.0. Affected is an unknown function of the file /admin/del_service.php. The manipulation of the argument editid 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-235242 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3880**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	7.5	A vulnerability classified as critical was found in Campcodes Beauty Salon Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/forgot-password.php. The manipulation of the argument contactno 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-235243. **CVE ID : CVE-2023-3881**	N/A	A-CAM-BEAU-020823/63

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	7.5	A vulnerability, which was classified as critical, has been found in Campcodes Beauty Salon Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit-accepted-appointment.php. The manipulation of the argument contactno 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-235244. **CVE ID : CVE-2023-3882**	N/A	A-CAM-BEAU-020823/64
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/add-category.php. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public	N/A	A-CAM-BEAU-020823/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. The identifier VDB-235245 was assigned to this vulnerability. **CVE ID : CVE-2023-3883**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	A vulnerability has been found in Campcodes Beauty Salon Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/edit_product.php. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235246 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3884**	N/A	A-CAM-BEAU-020823/66
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	A vulnerability was found in Campcodes Beauty Salon Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/edit_category.php. The manipulation of the argument id leads to cross site	N/A	A-CAM-BEAU-020823/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripting. 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-235247. **CVE ID : CVE-2023-3885**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /admin/invoice.php. The manipulation of the argument inv_id 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-235248. **CVE ID : CVE-2023-3886**	N/A	A-CAM-BEAU-020823/68
Improper Neutralization of Input During Web Page Generation	25-Jul-2023	6.1	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown	N/A	A-CAM-BEAU-020823/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			functionality of the file /admin/search-appointment.php. The manipulation of the argument searchdata 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-235249 was assigned to this vulnerability. **CVE ID : CVE-2023-3887**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	A vulnerability was found in Campcodes Beauty Salon Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-235250 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3888**	N/A	A-CAM-BEAU-020823/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	A vulnerability classified as problematic has been found in Campcodes Beauty Salon Management System 1.0. This affects an unknown part of the file /admin/edit-accepted-appointment.php. The manipulation of the argument id 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-235251. **CVE ID : CVE-2023-3890**	N/A	A-CAM-BEAU-020823/71
Affected Version(s): 0.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	7.5	A vulnerability has been found in Campcodes Beauty Salon Management System 0.1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/del_feedback.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public	N/A	A-CAM-BEAU-020823/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and may be used. The identifier VDB-235237 was assigned to this vulnerability. **CVE ID : CVE-2023-3875**		
Vendor: cdwanjiang					
Product: flash_flood_disaster_monitoring_and_warning_system					
Affected Version(s): 2.0					
Unrestricted Upload of File with Dangerous Type	20-Jul-2023	9.8	A vulnerability has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0 and classified as critical. This vulnerability affects unknown code of the file /App_Resource/UEditor/server/upload.aspx. The manipulation of the argument file leads to unrestricted upload. The exploit has been disclosed to the public and may be used. VDB-235066 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3798**	N/A	A-CDW-FLAS-020823/73
Unrestricted Upload of File with	21-Jul-2023	9.8	A vulnerability classified as problematic was found in Chengdu Flash Flood Disaster	N/A	A-CDW-FLAS-020823/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Monitoring and Warning System 2.0. This vulnerability affects unknown code of the file /Service/FileHandler.ashx. The manipulation of the argument userFile leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235072. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3804**		
Unrestricted Upload of File with Dangerous Type	21-Jul-2023	3.7	A vulnerability classified as problematic has been found in Chengdu Flash Flood Disaster Monitoring and Warning System 2.0. This affects an unknown part of the file /Service/ImageStationDataService.asmx of the component File Name Handler. The manipulation leads to insufficiently random values. The complexity of an attack is rather high. The exploitability is	N/A	A-CDW-FLAS-020823/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			told to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235071. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3803**		
Vendor: cern					
Product: indico					
Affected Version(s): * Up to (excluding) 3.2.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2023	5.4	Indico is an open source a general-purpose, web based event management tool. There is a Cross-Site-Scripting vulnerability in confirmation prompts commonly used when deleting content from Indico. Exploitation requires someone with at least submission privileges (such as a speaker) and then someone else to attempt to delete this content. Considering that event organizers may want to delete suspicious-looking content when spotting it, there is a non-negligible risk of such an attack to	https://github.com/indico/indico/security/advisories/GHSA-fmqq-25x9-c6hm, https://github.com/indico/indico/commit/2ee636d318653fb1ab193803dafbfe3e371d4130	A-CER-INDI-020823/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			succeed. The risk of this could be further increased when combined with some some social engineering pointing the victim towards this content. Users need to update to Indico 3.2.6 as soon as possible. See the docs for instructions on how to update. Users who cannot upgrade should only let trustworthy users manage categories, create events or upload materials ("submission" privileges on a contribution/event). This should already be the case in a properly-configured setup when it comes to category/event management. Note that a conference doing a Call for Abstracts actively invites external speakers (who the organizers may not know and thus cannot fully trust) to submit content, hence the need to update to a a fixed version ASAP in particular when using such workflows. **CVE ID : CVE-2023-37901**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Citrix					
Product: netscaler_application_delivery_controller					
Affected Version(s): 11.1-65.22					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	9.8	Unauthenticated remote code execution **CVE ID : CVE-2023-3519**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/77
N/A	19-Jul-2023	8	Privilege Escalation to root administrator (nsroot) **CVE ID : CVE-2023-3467**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/78
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	Reflected Cross-Site Scripting (XSS) **CVE ID : CVE-2023-3466**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-	A-CIT-NETS-020823/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cve20233519-cve20233466-cve20233467	
Affected Version(s): From (including) 12.1 Up to (excluding) 12.1-55.297					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	9.8	Unauthenticated remote code execution **CVE ID : CVE-2023-3519**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/80
N/A	19-Jul-2023	8	Privilege Escalation to root administrator (nsroot) **CVE ID : CVE-2023-3467**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/81
Improper Neutralization of Input During Web Page	19-Jul-2023	6.1	Reflected Cross-Site Scripting (XSS) **CVE ID : CVE-2023-3466**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-	A-CIT-NETS-020823/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')				gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-91.13					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	9.8	Unauthenticated remote code execution **CVE ID : CVE-2023-3519**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	A-CIT-NETS-020823/83
N/A	19-Jul-2023	8	Privilege Escalation to root administrator (nsroot) **CVE ID : CVE-2023-3467**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	A-CIT-NETS-020823/84
Improper Neutralization of	19-Jul-2023	6.1	Reflected Cross-Site Scripting (XSS)	https://support.citrix.com/article/C	A-CIT-NETS-020823/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-3466**	TX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-37.159					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	9.8	Unauthenticated remote code execution **CVE ID : CVE-2023-3519**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	A-CIT-NETS-020823/86
N/A	19-Jul-2023	8	Privilege Escalation to root administrator (nsroot) **CVE ID : CVE-2023-3467**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	A-CIT-NETS-020823/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	Reflected Cross-Site Scripting (XSS) **CVE ID : CVE-2023-3466**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	A-CIT-NETS-020823/88
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-49.13					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	9.8	Unauthenticated remote code execution **CVE ID : CVE-2023-3519**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346 6-cve2023346 7	A-CIT-NETS-020823/89
N/A	19-Jul-2023	8	Privilege Escalation to root administrator (nsroot) **CVE ID : CVE-2023-3467**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve2023351 9-cve2023346	A-CIT-NETS-020823/90

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				6-cve20233467	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	Reflected Cross-Site Scripting (XSS) **CVE ID : CVE-2023-3466**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/91
Product: netscaler_gateway					
Affected Version(s): From (including) 13.0 Up to (excluding) 13.0-91.13					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	9.8	Unauthenticated remote code execution **CVE ID : CVE-2023-3519**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/92
N/A	19-Jul-2023	8	Privilege Escalation to root administrator (nsroot) **CVE ID : CVE-2023-3467**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-	A-CIT-NETS-020823/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				security-bulletin-for-cve20233519-cve20233466-cve20233467	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	Reflected Cross-Site Scripting (XSS) **CVE ID : CVE-2023-3466**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/94
Affected Version(s): From (including) 13.1 Up to (excluding) 13.1-49.13					
Improper Control of Generation of Code ('Code Injection')	19-Jul-2023	9.8	Unauthenticated remote code execution **CVE ID : CVE-2023-3519**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/95
N/A	19-Jul-2023	8	Privilege Escalation to root administrator (nsroot)	https://support.citrix.com/article/CTX561482/c	A-CIT-NETS-020823/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3467	itrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	Reflected Cross-Site Scripting (XSS) **CVE ID : CVE-2023-3466**	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467	A-CIT-NETS-020823/97
Vendor: codexin					
Product: media_library_helper					
Affected Version(s): * Up to (including) 1.2.0					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Media Library Helper plugin <= 1.2.0 versions. **CVE ID : CVE-2023-37386**	N/A	A-COD-MEDI-020823/98
Vendor: creativeitem					
Product: academy_lms					
Affected Version(s): 5.15					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	A vulnerability was found in Creativeitem Academy LMS 5.15. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /home/courses. The manipulation of the argument sort_by leads to cross site scripting. The attack may be launched remotely. VDB-234422 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3752**	N/A	A-CRE-ACAD-020823/99
Product: atlas					
Affected Version(s): 2.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	A vulnerability has been found in Creativeitem Atlas Business Directory Listing 2.13 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /home/filter_listings. The manipulation of the argument price-range leads to cross site scripting. The attack can be launched	N/A	A-CRE-ATLA-020823/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The associated identifier of this vulnerability is VDB-234427. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3755**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	A vulnerability was found in Creativeitem Atlas Business Directory Listing 2.13 and classified as problematic. Affected by this issue is some unknown functionality of the file /home/search. The manipulation of the argument search_string leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-234428. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3756**	N/A	A-CRE-ATLA-020823/101
Product: ekushey_project_manager					
Affected Version(s): 5.0					
Improper Neutralization of Input	19-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in Creativeitem	N/A	A-CRE-EKUS-020823/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Ekushey Project Manager CRM 5.0. Affected is an unknown function of the file /index.php/client/message/message_read/xxxxxxxx[random-msg-hash]. The manipulation of the argument message leads to cross site scripting. It is possible to launch the attack remotely. VDB-234426 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3754**		
Product: mastery_lms					
Affected Version(s): 1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	A vulnerability classified as problematic has been found in Creativeitem Mastery LMS 1.2. This affects an unknown part of the file /browse. The manipulation of the argument search/featured/recommended/skill leads to cross site scripting. It is possible to initiate the attack remotely. The associated	N/A	A-CRE-MAST-020823/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-234423. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3753**		
Vendor: crudlab					
Product: jazz_popups					
Affected Version(s): * Up to (including) 1.8.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CRUDLab Jazz Popups plugin <= 1.8.7 versions. **CVE ID : CVE-2023-32965**	N/A	A-CRU-JAZZ-020823/104
Vendor: cththemes					
Product: balkon					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cththemes Balkon plugin <= 1.3.2 versions. **CVE ID : CVE-2023-36502**	N/A	A-CTH-BALK-020823/105
Vendor: custom_post_type_generator_project					
Product: custom_post_type_generator					
Affected Version(s): * Up to (including) 2.4.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	4.8	Auth. (admin+) Reflected Cross-Site Scripting (XSS) vulnerability in Hijiri Custom Post Type Generator plugin <= 2.4.2 versions. **CVE ID : CVE-2023-33329**	N/A	A-CUS-CUST-020823/106
Vendor: Dahuasecurity					
Product: smart_parking_management					
Affected Version(s): * Up to (including) 20230713					
Unrestricted Upload of File with Dangerous Type	22-Jul-2023	9.8	A vulnerability classified as critical was found in Dahua Smart Park Management up to 20230713. This vulnerability affects unknown code of the file /emap/devicePoint_addImgIco?hasSubsystem=true. The manipulation of the argument upload leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235162 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3836**	N/A	A-DAH-SMAR-020823/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: dedebiz					
Product: dedebiz					
Affected Version(s): 6.2.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jul-2023	7.2	A vulnerability, which was classified as problematic, has been found in DedeBIZ 6.2.10. Affected by this issue is some unknown functionality of the file /admin/sys_sql_query.php. The manipulation of the argument sqlquery leads to sql injection. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. VDB-235190 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3839**	N/A	A-DED-DEDE-020823/108
Improper Neutralization of Input During Web Page Generation	22-Jul-2023	4.8	A vulnerability classified as problematic has been found in DedeBIZ 6.2.10. Affected is an unknown function of the file	N/A	A-DED-DEDE-020823/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			/admin/sys_sql_query.php. The manipulation 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-235188. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3837**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	4.8	A vulnerability classified as problematic was found in DedeBIZ 6.2.10. Affected by this vulnerability is an unknown functionality of the file /admin/vote_edit.php. The manipulation 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-235189 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-DED-DEDE-020823/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3838		
Vendor: Dell					
Product: hybrid_client					
Affected Version(s): 2.0					
Exposure of Sensitive Information to an Unauthorized Actor	20-Jul-2023	5.5	Dell Hybrid Client version 2.0 contains a Sensitive Data Exposure vulnerability. An unauthenticated malicious user on the device can access hard coded secrets in javascript files. **CVE ID : CVE-2023-32476**	https://www.dell.com/support/kbdoc/en-us/000215862/dsa-2023-258-dell	A-DEL-HYBR-020823/111
Product: wyse_management_suite					
Affected Version(s): * Up to (excluding) 4.0					
Allocation of Resources Without Limits or Throttling	20-Jul-2023	6.5	Wyse Management Suite versions prior to 4.0 contain a denial-of-service vulnerability. An authenticated malicious user can flood the configured SMTP server with numerous requests in order to deny access to the system. **CVE ID : CVE-2023-32481**	https://www.dell.com/support/kbdoc/en-us/000215351/dsa-2023-240-dell-wyse-management-suite	A-DEL-WYSE-020823/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Jul-2023	4.9	Wyse Management Suite versions prior to 4.0 contain an improper authorization vulnerability. An authenticated malicious user with privileged access can push policies to unauthorized tenant group. **CVE ID : CVE-2023-32482**	https://www.dell.com/support/kbdoc/en-us/000215351/dsa-2023-240-dell-wyse-management-suite	A-DEL-WYSE-020823/113
Cleartext Storage of Sensitive Information	20-Jul-2023	4.4	Wyse Management Suite versions prior to 4.0 contain a sensitive information disclosure vulnerability. An authenticated malicious user having local access to the system running the application could exploit this vulnerability to read sensitive information written to log files. **CVE ID : CVE-2023-32483**	https://www.dell.com/support/kbdoc/en-us/000215351/dsa-2023-240-dell-wyse-management-suite	A-DEL-WYSE-020823/114
Vendor: deothemes					
Product: medikaid					
Affected Version(s): * Up to (excluding) 1.1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	6.1	Several themes for WordPress by DeoThemes are vulnerable to Reflected Cross-Site Scripting via breadcrumbs in various versions due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-3708**	https://themes.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=196758%40everse&new=196758%40everse&sfp_email=&sfph_mail=	A-DEO-MEDI-020823/115
Vendor: Diafan					
Product: diafan.cms					
Affected Version(s): 6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	6.1	Diafan CMS v6.0 was discovered to contain a reflected cross-site scripting via the cat_id parameter at /shop/?module=shop&action=search. **CVE ID : CVE-2023-37164**	N/A	A-DIA-DIAF-020823/116
Vendor: dijital					
Product: zekiweb					
Affected Version(s): * Up to (excluding) 2.0					
Improper Neutralization of	17-Jul-2023	9.8	Improper Neutralization of Special Elements used	N/A	A-DIJ-ZEKI-020823/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			in an SQL Command ('SQL Injection') vulnerability in Digital Strategy Zekiweb allows SQL Injection.This issue affects Zekiweb: before 2. **CVE ID : CVE-2023-3376**		
Vendor: drop_shadow_boxes_project					
Product: drop_shadow_boxes					
Affected Version(s): * Up to (including) 1.7.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Steven Henty Drop Shadow Boxes plugin <= 1.7.10 versions. **CVE ID : CVE-2023-23833**	N/A	A-DRO-DROP-020823/118
Vendor: easyappointments					
Product: easyappointments					
Affected Version(s): * Up to (excluding) 1.5.0					
Authorization Bypass Through User-Controlled Key	17-Jul-2023	4.3	Improper Access Control in GitHub repository alextselegidis/easyappointments prior to 1.5.0. **CVE ID : CVE-2023-3700**	https://huntr.dev/bounties/e8d530db-a6a7-4f79-a95d-b77654cc04f8, https://github.com/alextselegidis/easyappointments/commit/b37b460195	A-EAS-EASY-020823/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				53089db4f22eb2fe998bca84b2cb64	
Vendor: easy_captcha_project					
Product: easy_captcha					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wppal Easy Captcha plugin <= 1.0 versions. **CVE ID : CVE-2023-33312**	N/A	A-EAS-EASY-020823/120
Vendor: edinet-fsa					
Product: xbrl_data_create					
Affected Version(s): * Up to (including) 7.0					
Improper Restriction of XML External Entity Reference	19-Jul-2023	5.5	XBRL data create application version 7.0 and earlier improperly restricts XML external entity references (XXE). By processing a specially crafted XBRL file, arbitrary files on the system may be read by an attacker. **CVE ID : CVE-2023-32635**	N/A	A-EDI-XBRL-020823/121
Vendor: emlog					
Product: emlog					
Affected Version(s): 2.1.9					
Missing Authorization	26-Jul-2023	6.5	emlog 2.1.9 is vulnerable to Arbitrary file deletion via admin\template.php.	https://github.com/Num-Nine/CVE/issues/1	A-EML-EMLO-020823/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37049		
Vendor: emqx					
Product: emqx					
Affected Version(s): 4.3.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-2023	6.5	An issue in the emqx_sn plugin of EMQX v4.3.8 allows attackers to execute a directory traversal via uploading a crafted .txt file. **CVE ID : CVE-2023-37781**	https://github.com/emqx/emqx/issues/10419	A-EMQ-EMQX-020823/123
Vendor: Endonesia					
Product: endonesia					
Affected Version(s): 8.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jul-2023	9.8	SQL injection vulnerability in diskusi.php in eNdonesia 8.7, allows an attacker to execute arbitrary SQL commands via the "rid=" parameter. **CVE ID : CVE-2023-31753**	https://github.com/khmk2k/CVE-2023-31753/	A-END-ENDO-020823/124
Vendor: es					
Product: iperf3					
Affected Version(s): * Up to (excluding) 3.14					
Integer Overflow or Wraparound	17-Jul-2023	5.5	iperf3 before 3.14 allows peers to cause an integer overflow and heap corruption via a crafted length field. **CVE ID : CVE-2023-38403**	https://github.com/esnet/iperf/commit/0ef151550d96cc4460f98832df84b4a1e87c65e9, https://githu	A-ES-IPER-020823/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b.com/esnet/iperf/issues/1542, https://downloads.es.net/pub/iperf/esnet-secadv-2023-0001.txt.asc	
Vendor: Esri					
Product: arcgis_insights					
Affected Version(s): 2022.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2023	7.5	There is SQL injection vulnerability in Esri ArcGIS Insights 2022.1 for ArcGIS Enterprise and that may allow a remote, authorized attacker to execute arbitrary SQL commands against the back-end database. The effort required to generate the crafted input required to exploit this issue is complex and requires significant effort before a successful attack can be expected. **CVE ID : CVE-2023-25838**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-insights-security-patches-for-arcgis-insights-2022-1-are-now-available/	A-ESR-ARCG-020823/126
Improper Neutralization of Special Elements used in an SQL Command	19-Jul-2023	7	There is SQL injection vulnerability in Esri ArcGIS Insights Desktop for Mac and Windows version 2022.1 that may allow	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-insights-	A-ESR-ARCG-020823/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			a local, authorized attacker to execute arbitrary SQL commands against the back-end database. The effort required to generate the crafted input required to exploit this issue is complex and requires significant effort before a successful attack can be expected. **CVE ID : CVE-2023-25839**	security-patches-for-arcgis-insights-2022-1-are-now-available/	
Product: portal_for_arcgis					
Affected Version(s): From (including) 10.8.1 Up to (including) 10.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2023	5.4	There is a Cross-site Scripting vulnerability in Esri Portal Sites in versions 10.8.1 – 10.9 that may allow a remote, authenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victims browser. The privileges required to execute this attack are high. **CVE ID : CVE-2023-25837**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-enterprise-sites-security-patch-is-now-available/	A-ESR-PORT-020823/128
Affected Version(s): From (including) 10.8.1 Up to (including) 11.1					
Improper Neutralizat	21-Jul-2023	4.8		https://www.esri.com/a	A-ESR-PORT-020823/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			There is a Cross-site Scripting vulnerability in Esri Portal Sites in versions 10.8.1 – 11.1 that may allow a remote, authenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victims browser. The privileges required to execute this attack are high. **CVE ID : CVE-2023-25835**	rcgis-blog/products/trust-arcgis/administration/portal-for-arcgis-enterprise-sites-security-patch-is-now-available/	
Vendor: ethyca					
Product: fides					
Affected Version(s): From (including) 2.11.0 Up to (excluding) 2.16.0					
Uncontrolled Resource Consumption	18-Jul-2023	4.9	Fides is an open-source privacy engineering platform for managing data privacy requests and privacy regulations. The Fides webserver is vulnerable to a type of Denial of Service (DoS) attack. Attackers can exploit a weakness in the connector template upload feature to upload a malicious zip bomb file, resulting in resource exhaustion and service unavailability for all users of the Fides	https://github.com/ethyca/fides/commit/5aea738463960d81821c11ae7ade1d627a46bf32	A-ETH-FIDE-020823/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webserver. This vulnerability affects Fides versions `2.11.0` through `2.15.1`. Exploitation is limited to users with elevated privileges with the `CONNECTOR_TEMPLATE_REGISTER` scope, which includes root users and users with the owner role. The vulnerability has been patched in Fides version `2.16.0`. Users are advised to upgrade to this version or later to secure their systems against this threat. There is no known workaround to remediate this vulnerability without upgrading. If an attack occurs, the impact can be mitigated by manually or automatically restarting the affected container. **CVE ID : CVE-2023-37480**		
Uncontrolled Resource Consumption	18-Jul-2023	4.9	Fides is an open-source privacy engineering platform for managing data privacy requests and privacy regulations. The Fides webserver is vulnerable to a type of Denial of Service (DoS) attack.	https://github.com/ethyca/fides/commit/8beaace082b325e693dc7682029a3cb7e6c2b69d, https://github.com/ethyc	A-ETH-FIDE-020823/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Attackers can exploit this vulnerability to upload zip files containing malicious SVG bombs (similar to a billion laughs attack), causing resource exhaustion in Admin UI browser tabs and creating a persistent denial of service of the 'new connector' page (`datastore-connection/new`). This vulnerability affects Fides versions `2.11.0` through `2.15.1`. Exploitation is limited to users with elevated privileges with the `CONNECTOR_TEMPLATE_REGISTER` scope, which includes root users and users with the owner role. The vulnerability has been patched in Fides version `2.16.0`. Users are advised to upgrade to this version or later to secure their systems against this threat. There is no known workaround to remediate this vulnerability without upgrading. **CVE ID : CVE-2023-37481**	a/fides/security/advisories/GHSA-3rw2-wfc8-wmj5	
Vendor: etoilewebdesign					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: front_end_users					
Affected Version(s): * Up to (including) 3.2.24					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Etoile Web Design Front End Users plugin <= 3.2.24 versions. **CVE ID : CVE-2023-34005**	N/A	A-ETO-FRON-020823/132
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): 1.6.3					
Exposure of Resource to Wrong Sphere	20-Jul-2023	5.3	eyoucms v1.6.3 was discovered to contain an information disclosure vulnerability via the component /custom_model_path/recruit.filelist.txt. **CVE ID : CVE-2023-37645**	N/A	A-EYO-EYOU-020823/133
Vendor: faboba					
Product: falang					
Affected Version(s): * Up to (including) 1.3.39					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Faboba Falang multilanguage for WordPress plugin <= 1.3.39 versions. **CVE ID : CVE-2023-37968**	N/A	A-FAB-FALA-020823/134
Vendor: feathersjs					
Product: feathers					
Affected Version(s): * Up to (excluding) 4.5.18					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	19-Jul-2023	7.5	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. Feathers socket handler did not catch invalid string conversion errors like `const message = ${{ toString: '' }}` which would cause the NodeJS process to crash when sending an unexpected Socket.io message like `socket.emit('find', { toString: '' })`. A fix has been released in versions 5.0.8 and 4.5.18. Users are advised to upgrade. There is no known workaround for this vulnerability. **CVE ID : CVE-2023-37899**	https://github.com/feathersjs/feathers/pull/3242, https://github.com/feathersjs/feathers/pull/3241, https://github.com/feathersjs/feathers/security/advisories/GHSA-hhr9-rh25-hvf9	A-FEA-FEAT-020823/135
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.8					
Improper Check for Unusual or Exceptional Conditions	19-Jul-2023	7.5	Feathersjs is a framework for creating web APIs and real-time applications with TypeScript or JavaScript. Feathers socket handler did not catch invalid string conversion errors like `const message = ${{ toString: '' }}` which would cause the NodeJS process to crash when sending an unexpected	https://github.com/feathersjs/feathers/pull/3242, https://github.com/feathersjs/feathers/pull/3241, https://github.com/feathersjs/feathers/security/advisories/GHSA-hhr9-rh25-hvf9	A-FEA-FEAT-020823/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Socket.io message like `socket.emit('find', { toString: '' })`. A fix has been released in versions 5.0.8 and 4.5.18. Users are advised to upgrade. There is no known workaround for this vulnerability. **CVE ID : CVE-2023-37899**		
Vendor: fit2cloud					
Product: 1panel					
Affected Version(s): * Up to (excluding) 1.4.3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Jul-2023	8.8	1Panel is an open source Linux server operation and maintenance management panel. An OS command injection vulnerability exists in 1Panel firewall functionality. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability. 1Panel firewall functionality `/hosts/firewall/ip` endpoint read user input without validation, the attacker extends the default functionality of the application, which execute system commands. An	https://github.com/1Panel-dev/1Panel/commit/e17b80cff4975ee343568ff526b62319f499005d, https://github.com/1Panel-dev/1Panel/security/advisories/GHSA-p9xf-74xh-mhw5	A-FIT-1PAN-020823/137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can execute arbitrary code on the target system, which can lead to a complete compromise of the system. This issue has been addressed in commit `e17b80cff49` which is included in release version `1.4.3`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37477**		
Product: kubepi					
Affected Version(s): * Up to (excluding) 1.6.5					
N/A	21-Jul-2023	8.8	KubePi is an opensource kubernetes management panel. A normal user has permission to create/update users, they can become admin by editing the `isadmin` value in the request. As a result any user may take administrative control of KubePi. This issue has been addressed in version 1.6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37917**	N/A	A-FIT-KUBE-020823/138
N/A	21-Jul-2023	7.5	KubePi is an opensource	N/A	A-FIT-KUBE-020823/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kubernetes management panel. The endpoint /kubepi/api/v1/users /search?pageNum=1& &pageSize=10 leak password hash of any user (including admin). A sufficiently motivated attacker may be able to crack leaded password hashes. This issue has been addressed in version 1.6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37916**		
Vendor: fivestarplugins					
Product: five_star_restaurant_menu					
Affected Version(s): * Up to (excluding) 2.4.7					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in FiveStarPlugins Restaurant Menu and Food Ordering plugin <= 2.4.6 versions. **CVE ID : CVE-2023-37985**	N/A	A-FIV-FIVE-020823/140
Affected Version(s): * Up to (including) 2.6.7					
Improper Neutralization of Input During Web Page Generation	25-Jul-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FiveStarPlugins Five Star Restaurant Reservations plugin <= 2.6.7 versions.	N/A	A-FIV-FIVE-020823/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-34017**		
Vendor: flickr_justified_gallery_project					
Product: flickr_justified_gallery					
Affected Version(s): * Up to (including) 3.5					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Miro Mannino Flickr Justified Gallery plugin <= 3.5 versions. **CVE ID : CVE-2023-25473**	N/A	A-FLI-FLIC-020823/142
Vendor: four-faith					
Product: video_surveillance_management_system					
Affected Version(s): * Up to (including) 2023-07-12					
Improper Authorization	21-Jul-2023	9.8	A vulnerability, which was classified as critical, has been found in Xiamen Four Letter Video Surveillance Management System up to 20230712. This issue affects some unknown processing in the library UserInfoAction.class of the component Login. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235073 was assigned to this vulnerability. NOTE:	N/A	A-FOU-VIDE-020823/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3805**		
Vendor: Foxit					
Product: pdf_reader					
Affected Version(s): 12.1.1.15289					
Use After Free	19-Jul-2023	8.8	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.1.1.15289. A specially crafted PDF document can trigger the reuse of previously freed memory by manipulating form fields of a specific type. This can lead to memory corruption and arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. **CVE ID : CVE-2023-28744**	N/A	A-FOX-PDF_-020823/144
Affected Version(s): 12.1.2.15332					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Jul-2023	8.8	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.1.2.15332. By prematurely deleting objects associated with pages, a specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. **CVE ID : CVE-2023-27379**	N/A	A-FOX-PDF_-020823/145
Use After Free	19-Jul-2023	8.8	A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 12.1.2.15332. By prematurely deleting objects associated with pages, a specially crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker	N/A	A-FOX-PDF_-020823/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needs to trick the user into opening the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially crafted, malicious site if the browser plugin extension is enabled. **CVE ID : CVE-2023-33866**		
Use After Free	19-Jul-2023	8.8	A use-after-free vulnerability exists in the way Foxit Reader 12.1.2.15332 handles destroying annotations. A specially-crafted Javascript code inside a malicious PDF document can trigger reuse of a previously freed object which can lead to memory corruption and result in arbitrary code execution. A specially-crafted Javascript code inside a malicious PDF document can cause memory corruption and lead to remote code execution. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled. **CVE ID : CVE-2023-33876**	N/A	A-FOX-PDF_-020823/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	19-Jul-2023	7.8	A type confusion vulnerability exists in the Javascript checkThisBox method as implemented in Foxit Reader 12.1.2.15332. A specially-crafted Javascript code inside a malicious PDF document can cause memory corruption and lead to remote code execution. User would need to open a malicious file to trigger the vulnerability. **CVE ID : CVE-2023-32664**	N/A	A-FOX-PDF_-020823/148
Vendor: GE					
Product: cimplicity					
Affected Version(s): *					
Out-of-bounds Write	19-Jul-2023	9.8	All versions of GE Digital CIMPLICITY that are not adhering to SDG guidance and accepting documents from untrusted sources are vulnerable to memory corruption issues due to insufficient input validation, including issues such as out-of-bounds reads and writes, use-after-free, stack-based buffer overflows, uninitialized pointers, and a heap-based	N/A	A-GE-CIMP-020823/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. Successful exploitation could allow an attacker to execute arbitrary code. **CVE ID : CVE-2023-3463**		
Vendor: getgrav					
Product: grav					
Affected Version(s): 1.7.42					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-Jul-2023	8.8	Grav is a file-based Web-platform built in PHP. Grav is subject to a server side template injection (SSTI) vulnerability. The fix for another SSTI vulnerability using `|map`, `|filter` and `|reduce` twigs implemented in the commit `71bbed1` introduces bypass of the denylist due to incorrect return value from `isDangerousFunction()`, which allows to execute the payload prepending double backslash (`\\`). The `isDangerousFunction()` check in version 1.7.42 and onwards retuns `false` value instead of `true` when the `\` symbol is found in the `$name`. This vulnerability can be exploited if the attacker has access to:	https://github.com/getgrav/grav/commit/b4c62101a43051fc7f5349c7d0a5b6085375c1d7, https://github.com/getgrav/grav/security/advisories/GHSA-9436-3gmp-4f53	A-GET-GRAV-020823/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1. an Administrator account, or 2. a non-administrator, user account that has Admin panel access and Create/Update page permissions. A fix for this vulnerability has been introduced in commit `b4c6210` and is included in release version `1.7.42.2`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37897**		
Affected Version(s): 1.7.42.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-Jul-2023	8.8	Grav is a file-based Web-platform built in PHP. Grav is subject to a server side template injection (SSTI) vulnerability. The fix for another SSTI vulnerability using `|map`, `|filter` and `|reduce` twigs implemented in the commit `71bbed1` introduces bypass of the denylist due to incorrect return value from `isDangerousFunction()`, which allows to execute the payload prepending double backslash (`\\`). The `isDangerousFunction()` check in version	https://github.com/getgrav/grav/commit/b4c62101a43051fc7f5349c7d0a5b6085375c1d7, https://github.com/getgrav/grav/security/advisories/GHSA-9436-3gmp-4f53	A-GET-GRAV-020823/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.7.42 and onwards retuns `false` value instead of `true` when the `\` symbol is found in the `$name`. This vulnerability can be exploited if the attacker has access to: 1. an Administrator account, or 2. a non-administrator, user account that has Admin panel access and Create/Update page permissions. A fix for this vulnerability has been introduced in commit `b4c6210` and is included in release version `1.7.42.2`. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37897**		
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): 16.1.0					
N/A	21-Jul-2023	5.3	A sensitive information leak issue has been discovered in GitLab EE affecting all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1, which allows access to titles of private issue and MR.	N/A	A-GIT-GITL-020823/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3102		
Affected Version(s): From (including) 12.8.0 Up to (excluding) 15.11.11					
N/A	21-Jul-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 12.8 before 15.11.11, all versions starting from 16.0 before 16.0.7, all versions starting from 16.1 before 16.1.2. An attacker could change the name or path of a public top-level group in certain situations. **CVE ID : CVE-2023-3484**	https://about.gitlab.com/releases/2023/07/05/security-release-gitlab-16-1-2-released/	A-GIT-GITL-020823/153
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.6					
N/A	21-Jul-2023	5.3	A sensitive information leak issue has been discovered in GitLab EE affecting all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1, which allows access to titles of private issue and MR. **CVE ID : CVE-2023-3102**	N/A	A-GIT-GITL-020823/154
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.0.7					
N/A	21-Jul-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 12.8 before 15.11.11, all versions starting from 16.0 before	https://about.gitlab.com/releases/2023/07/05/security-release-	A-GIT-GITL-020823/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			16.0.7, all versions starting from 16.1 before 16.1.2. An attacker could change the name or path of a public top-level group in certain situations. **CVE ID : CVE-2023-3484**	gitlab-16-1-2-released/	
Affected Version(s): From (including) 16.1.0 Up to (excluding) 16.1.2					
N/A	21-Jul-2023	6.5	An issue has been discovered in GitLab EE affecting all versions starting from 12.8 before 15.11.11, all versions starting from 16.0 before 16.0.7, all versions starting from 16.1 before 16.1.2. An attacker could change the name or path of a public top-level group in certain situations. **CVE ID : CVE-2023-3484**	https://about.gitlab.com/releases/2023/07/05/security-release-gitlab-16-1-2-released/	A-GIT-GITL-020823/156
Vendor: goproxy_project					
Product: goproxy					
Affected Version(s): 1.1					
Uncontrolled Resource Consumption	18-Jul-2023	7.5	goproxy v1.1 was discovered to contain an issue which can lead to a Denial of service (DoS) via unspecified vectors. **CVE ID : CVE-2023-37788**	N/A	A-GOP-GOPR-020823/157
Vendor: grame					
Product: faust					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Jul-2023	5.5	faust commit ee39a19 was discovered to contain a stack overflow via the component boxppShared::print() at /boxes/ppbox.cpp. **CVE ID : CVE-2023-37770**	https://github.com/grame-cncm/faust/issues/922	A-GRA-FAUS-020823/158
Vendor: gsheetconnector					
Product: caldera_forms_google_sheets_connector					
Affected Version(s): * Up to (including) 1.2					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	The Caldera Forms Google Sheets Connector WordPress plugin through 1.2 does not have CSRF check when updating its Access Code, which could allow attackers to make logged in admin change the access code to an arbitrary one via a CSRF attack **CVE ID : CVE-2023-2330**	N/A	A-GSH-CALD-020823/159
Product: woocommerce_google_sheet_connector					
Affected Version(s): * Up to (including) 1.3.4					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	The WooCommerce Google Sheet Connector WordPress plugin through 1.3.4 does not have CSRF check when updating its Access Code, which could allow attackers to make logged in admin change the access code to an	N/A	A-GSH-WOOC-020823/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary one via a CSRF attack **CVE ID : CVE-2023-2329**		
Vendor: gss					
Product: vitals_enterprise_social_platform					
Affected Version(s): From (including) 3.0.8 Up to (including) 6.2.0					
Use of Hard-coded Credentials	21-Jul-2023	9.8	Galaxy Software Services Vitals ESP is vulnerable to using a hard-coded encryption key. An unauthenticated remote attacker can generate a valid token parameter and exploit this vulnerability to access system to operate processes and access data. This issue affects Vitals ESP: from 3.0.8 through 6.2.0. **CVE ID : CVE-2023-37291**	N/A	A-GSS-VITA-020823/161
Vendor: gvectors					
Product: wpforo_forum					
Affected Version(s): * Up to (excluding) 2.1.9					
Improper Neutralization of Input During Web Page Generation	24-Jul-2023	6.1	The wpForo Forum WordPress plugin before 2.1.9 does not escape some request parameters while in debug mode, leading to a Reflected Cross-	N/A	A-GVE-WPFO-020823/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Site Scripting vulnerability. **CVE ID : CVE-2023-2309**		
Vendor: gzscripts					
Product: car_rental_php_script					
Affected Version(s): 1.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	A vulnerability classified as problematic has been found in GZ Scripts Car Rental Script 1.8. Affected is an unknown function of the file /EventBookingCalendar/load.php?controller=GzFront/action=checkout/cid=1/layout=calendar/show_header=T/local=3. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-234432. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3757**	N/A	A-GZS-CAR_-020823/163
Vendor: hashicorp					
Product: nomad					
Affected Version(s): From (including) 0.11.0 Up to (including) 1.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	20-Jul-2023	5.3	HashiCorp Nomad and Nomad Enterprise 0.11.0 up to 1.5.6 and 1.4.1 HTTP search API can reveal names of available CSI plugins to unauthenticated users or users without the plugin:read policy. Fixed in 1.6.0, 1.5.7, and 1.4.1. **CVE ID : CVE-2023-3300**	https://discuss.hashicorp.com/t/hcsec-2023-22-nomad-search-api-leaks-information-about-csi-plugins/56272	A-HAS-NOMA-020823/164
Affected Version(s): From (including) 0.7.0 Up to (including) 1.4.10					
Missing Authorization	20-Jul-2023	3.8	HashiCorp Nomad and Nomad Enterprise 0.7.0 up to 1.5.6 and 1.4.10 ACL policies using a block without a label generates unexpected results. Fixed in 1.6.0, 1.5.7, and 1.4.11. **CVE ID : CVE-2023-3072**	https://discuss.hashicorp.com/t/hcsec-2023-20-nomad-acl-policies-without-label-are-applied-to-unexpected-resources/56270	A-HAS-NOMA-020823/165
Affected Version(s): From (including) 1.2.11 Up to (including) 1.4.10					
Exposure of Resource to Wrong Sphere	20-Jul-2023	2.7	HashiCorp Nomad Enterprise 1.2.11 up to 1.5.6, and 1.4.10 ACL policies using a block without a label generates unexpected results. Fixed in 1.6.0, 1.5.7, and 1.4.11. **CVE ID : CVE-2023-3299**	https://discuss.hashicorp.com/t/hcsec-2023-21-nomad-caller-acl-tokens-secret-id-is-exposed-to-sentinel/56271	A-HAS-NOMA-020823/166
Affected Version(s): From (including) 1.5.0 Up to (including) 1.5.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	20-Jul-2023	5.3	HashiCorp Nomad and Nomad Enterprise 0.11.0 up to 1.5.6 and 1.4.1 HTTP search API can reveal names of available CSI plugins to unauthenticated users or users without the plugin:read policy. Fixed in 1.6.0, 1.5.7, and 1.4.1. **CVE ID : CVE-2023-3300**	https://discuss.hashicorp.com/t/hcsec-2023-22-nomad-search-api-leaks-information-about-csi-plugins/56272	A-HAS-NOMA-020823/167
Missing Authorization	20-Jul-2023	3.8	HashiCorp Nomad and Nomad Enterprise 0.7.0 up to 1.5.6 and 1.4.10 ACL policies using a block without a label generates unexpected results. Fixed in 1.6.0, 1.5.7, and 1.4.11. **CVE ID : CVE-2023-3072**	https://discuss.hashicorp.com/t/hcsec-2023-20-nomad-acl-policies-without-label-are-applied-to-unexpected-resources/56270	A-HAS-NOMA-020823/168
Exposure of Resource to Wrong Sphere	20-Jul-2023	2.7	HashiCorp Nomad Enterprise 1.2.11 up to 1.5.6, and 1.4.10 ACL policies using a block without a label generates unexpected results. Fixed in 1.6.0, 1.5.7, and 1.4.11. **CVE ID : CVE-2023-3299**	https://discuss.hashicorp.com/t/hcsec-2023-21-nomad-caller-acl-tokens-secret-id-is-exposed-to-sentinel/56271	A-HAS-NOMA-020823/169
Vendor: hazelcast					
Product: hazelcast					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.0.5					
Missing Authorization	18-Jul-2023	8.8	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, executor services don't check client permissions properly, allowing authenticated users to execute tasks on members without the required permissions granted. **CVE ID : CVE-2023-33265**	https://support.hazelcast.com/s/article/Security-Advisory-for-CVE-2023-33265	A-HAZ-HAZE-020823/170
Affected Version(s): From (including) 5.1.0 Up to (excluding) 5.1.7					
Missing Authorization	18-Jul-2023	8.8	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, executor services don't check client permissions properly, allowing authenticated users to execute tasks on members without the required permissions granted. **CVE ID : CVE-2023-33265**	https://support.hazelcast.com/s/article/Security-Advisory-for-CVE-2023-33265	A-HAZ-HAZE-020823/171
Affected Version(s): From (including) 5.2.0 Up to (excluding) 5.2.4					
Missing Authorization	18-Jul-2023	8.8	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, executor services don't check client permissions properly, allowing authenticated users to execute tasks on members without the	https://support.hazelcast.com/s/article/Security-Advisory-for-CVE-2023-33265	A-HAZ-HAZE-020823/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			required permissions granted. **CVE ID : CVE-2023-33265**		
Product: imdg					
Affected Version(s): * Up to (including) 4.2					
Missing Authorization	18-Jul-2023	8.8	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, executor services don't check client permissions properly, allowing authenticated users to execute tasks on members without the required permissions granted. **CVE ID : CVE-2023-33265**	https://support.hazelcast.com/s/article/Security-Advisory-for-CVE-2023-33265	A-HAZ-IMDG-020823/173
Vendor: hcltech					
Product: bigfix_webui					
Affected Version(s): -					
Inadequate Encryption Strength	18-Jul-2023	7.5	The BigFix WebUI uses weak cipher suites. **CVE ID : CVE-2023-28021**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106123	A-HCL-BIGF-020823/174
URL Redirection to Untrusted Site ('Open Redirect')	18-Jul-2023	6.1	URL redirection in Login page in HCL BigFix WebUI allows malicious user to redirect the client browser to an external site via redirect URL response header. **CVE ID : CVE-2023-28020**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106123	A-HCL-BIGF-020823/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 14					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jul-2023	8.8	Insufficient validation in Bigfix WebUI API App site version < 14 allows an authenticated WebUI user to issue SQL queries via an unparameterized SQL query. **CVE ID : CVE-2023-28019**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106123	A-HCL-BIGF-020823/176
Affected Version(s): * Up to (including) 44					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	6.5	A cross site request forgery vulnerability in the BigFix WebUI Software Distribution interface site version 44 and before allows an NMO attacker to access files on server side systems (server machine and all the ones in its network). **CVE ID : CVE-2023-28023**	N/A	A-HCL-BIGF-020823/177
Vendor: Hitachi					
Product: device_manager					
Affected Version(s): * Up to (excluding) 8.8.5-02					
Improper Certificate Validation	18-Jul-2023	8.1	Improper Validation of Certificate with Host Mismatch vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Man in the	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-125/index.html	A-HIT-DEVI-020823/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Middle Attack.This issue affects Hitachi Device Manager: before 8.8.5-02. **CVE ID : CVE-2023-34143**		
Cleartext Transmission of Sensitive Information	18-Jul-2023	7.5	Cleartext Transmission of Sensitive Information vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Interception.This issue affects Hitachi Device Manager: before 8.8.5-02. **CVE ID : CVE-2023-34142**	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-125/index.html	A-HIT-DEVI-020823/179
Vendor: hospital_management_system_project					
Product: hospital_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jul-2023	9.8	A vulnerability was found in Hospital Management System 1.0. It has been classified as critical. This affects an unknown part of the file patient.php. The manipulation of the argument address leads to sql injection. It is possible to initiate the attack remotely.	N/A	A-HOS-HOSP-020823/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The identifier VDB-235077 was assigned to this vulnerability. **CVE ID : CVE-2023-3809**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jul-2023	9.8	A vulnerability was found in Hospital Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file patientappointment.php. The manipulation of the argument loginid/password/mobileno/appointmentdate/appointmenttime/patiente/dob/doct/city leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235078 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3810**	N/A	A-HOS-HOSP-020823/181
Improper Neutralization of Special Elements used in an SQL Command	21-Jul-2023	9.8	A vulnerability was found in Hospital Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file patientprofile.php. The manipulation of	N/A	A-HOS-HOSP-020823/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			the argument address 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-235079. **CVE ID : CVE-2023-3811**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jul-2023	8.8	A vulnerability was found in Hospital Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file patientforgotpassword.php. The manipulation 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-235076. **CVE ID : CVE-2023-3808**	N/A	A-HOS-HOSP-020823/183
Vendor: house_rental_and_property_listing_php_project					
Product: house_rental_and_property_listing_php					
Affected Version(s): 1.0					
Unrestricted Upload of File with	21-Jul-2023	9.8	A vulnerability, which was classified as critical, was found in SourceCodester House Rental and Property	N/A	A-HOU-HOUS-020823/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Listing System 1.0. Affected is an unknown function of the file btn_functions.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-235074 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3806**		
Vendor: hpe					
Product: intelligent_provisioning					
Affected Version(s): * Up to (excluding) 2.87					
N/A	18-Jul-2023	7.8	The vulnerability could be locally exploited to allow escalation of privilege. **CVE ID : CVE-2023-30906**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04486en_us	A-HPE-INTE-020823/185
Vendor: iagona					
Product: scrutisweb					
Affected Version(s): * Up to (including) 2.1.37					
Unrestricted Upload of File with Dangerous Type	18-Jul-2023	9.8	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to a remote code execution vulnerability that could allow an unauthenticated user to	N/A	A-IAG-SCRU-020823/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload a malicious payload and execute it. **CVE ID : CVE-2023-35189**		
Absolute Path Traversal	18-Jul-2023	7.5	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to a directory traversal vulnerability that could allow an unauthenticated user to directly access any file outside the webroot. **CVE ID : CVE-2023-33871**	N/A	A-IAG-SCRU-020823/187
Authorization Bypass Through User-Controlled Key	18-Jul-2023	7.5	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to an insecure direct object reference vulnerability that could allow an unauthenticated user to view profile information, including user login names and encrypted passwords. **CVE ID : CVE-2023-38257**	N/A	A-IAG-SCRU-020823/188
Use of Hard-coded Credentials	18-Jul-2023	5.5	Iagona ScrutisWeb versions 2.1.37 and prior are vulnerable to a cryptographic vulnerability that could allow an unauthenticated user to decrypt encrypted passwords into plaintext.	N/A	A-IAG-SCRU-020823/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35763		
Vendor: IBM					
Product: cloud_pak_for_data					
Affected Version(s): 4.0					
Insertion of Sensitive Information into Log File	19-Jul-2023	7.5	Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to exploit this vulnerability to conduct further attacks. IBM X-Force ID: 247896. **CVE ID : CVE-2023-26023**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247896, https://www.ibm.com/support/pages/node/6999351	A-IBM-CLOU-020823/190
Insertion of Sensitive Information into Log File	19-Jul-2023	7.5	Planning Analytics Cartridge for Cloud Pak for Data 4.0 exposes sensitive information in logs which could lead an attacker to exploit this vulnerability to conduct further attacks. IBM X-Force ID: 247896. **CVE ID : CVE-2023-26026**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247896, https://www.ibm.com/support/pages/node/6999351	A-IBM-CLOU-020823/191
Improper Authentication	19-Jul-2023	7.5	IBM Planning Analytics Cartridge for Cloud Pak for Data 4.0 connects to a CouchDB server. An attacker can exploit an insecure password policy to the CouchDB server and collect sensitive information	https://www.ibm.com/support/pages/node/6999351, https://exchange.xforce.ibmcloud.com/vulnerabi	A-IBM-CLOU-020823/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the database. IBM X-Force ID: 247905. **CVE ID : CVE-2023-27877**	lities/247905	
Product: cognos_analytics					
Affected Version(s): 11.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 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: 247861. **CVE ID : CVE-2023-25929**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247861, https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/193
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal	https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim's cookie-based authentication credentials. IBM X-Force ID: 251214. **CVE ID : CVE-2023-28530**		
Affected Version(s): 11.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 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: 247861. **CVE ID : CVE-2023-25929**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247861, https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/195
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal	https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim's cookie-based authentication credentials. IBM X-Force ID: 251214. **CVE ID : CVE-2023-28530**		
Affected Version(s): From (including) 11.1.0 Up to (excluding) 11.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 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: 247861. **CVE ID : CVE-2023-25929**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247861, https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/197
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal	https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim's cookie-based authentication credentials. IBM X-Force ID: 251214. **CVE ID : CVE-2023-28530**		
Affected Version(s): From (including) 11.2.0 Up to (excluding) 11.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 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: 247861. **CVE ID : CVE-2023-25929**	https://exchange.xforce.ibmcloud.com/vulnerabilities/247861, https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/199
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-2023	5.4	IBM Cognos Analytics 11.1 and 11.2 is vulnerable to stored cross-site scripting, caused by improper validation of SVG Files in Custom Visualizations. A remote attacker could exploit this vulnerability to execute scripts in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal	https://www.ibm.com/support/pages/node/7012621	A-IBM-COGN-020823/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the victim's cookie-based authentication credentials. IBM X-Force ID: 251214. **CVE ID : CVE-2023-28530**		
Product: db2					
Affected Version(s): 11.5					
Out-of-bounds Write	17-Jul-2023	6.7	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 with a Federated configuration is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user with SYSADM privileges could overflow the buffer and execute arbitrary code on the system. IBM X-Force ID: 257763. **CVE ID : CVE-2023-35012**	https://www.ibm.com/support/pages/node/7010747, https://exchange.xforce.ibmcloud.com/vulnerabilities/257763	A-IBM-DB2-020823/201
Product: i					
Affected Version(s): 7.2					
N/A	16-Jul-2023	7.8	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host	https://www.ibm.com/support/pages/node/7012355, https://exchange.xforce.ibmcloud.com/vulnerabilities/254016	A-IBM-I-020823/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operating system. IBM X-Force ID: 254016. **CVE ID : CVE-2023-30988**		
N/A	16-Jul-2023	7.8	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain all object access to the host operating system. IBM X-Force ID: 254017. **CVE ID : CVE-2023-30989**	https://www.ibm.com/support/pages/node/7012353, https://exchange.xforce.ibmcloud.com/vulnerabilities/254017	A-IBM-I-020823/203
Affected Version(s): 7.3					
N/A	16-Jul-2023	7.8	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host operating system. IBM X-Force ID: 254016. **CVE ID : CVE-2023-30988**	https://www.ibm.com/support/pages/node/7012355, https://exchange.xforce.ibmcloud.com/vulnerabilities/254016	A-IBM-I-020823/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Jul-2023	7.8	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain all object access to the host operating system. IBM X-Force ID: 254017. **CVE ID : CVE-2023-30989**	https://www.ibm.com/support/pages/node/7012353, https://exchange.xforce.ibmcloud.com/vulnerabilities/254017	A-IBM-I-020823/205
Affected Version(s): 7.4					
N/A	16-Jul-2023	7.8	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host operating system. IBM X-Force ID: 254016. **CVE ID : CVE-2023-30988**	https://www.ibm.com/support/pages/node/7012355, https://exchange.xforce.ibmcloud.com/vulnerabilities/254016	A-IBM-I-020823/206
N/A	16-Jul-2023	7.8	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability. A malicious actor with	https://www.ibm.com/support/pages/node/7012353, https://exchange.xforce.i	A-IBM-I-020823/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command line access to the host operating system can elevate privileges to gain all object access to the host operating system. IBM X-Force ID: 254017. **CVE ID : CVE-2023-30989**	bmcloud.com/vulnerabilities/254017	
Affected Version(s): 7.5					
N/A	16-Jul-2023	7.8	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host operating system. IBM X-Force ID: 254016. **CVE ID : CVE-2023-30988**	https://www.ibm.com/support/pages/node/7012355, https://exchange.xforce.ibmcloud.com/vulnerabilities/254016	A-IBM-I-020823/208
N/A	16-Jul-2023	7.8	IBM Performance Tools for i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain all object access to the host operating system.	https://www.ibm.com/support/pages/node/7012353, https://exchange.xforce.ibmcloud.com/vulnerabilities/254017	A-IBM-I-020823/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 254017. **CVE ID : CVE-2023-30989**		
Product: infosphere_information_server					
Affected Version(s): 11.7					
N/A	19-Jul-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information due to an insecure security configuration in InfoSphere Data Flow Designer. IBM X-Force ID: 259352. **CVE ID : CVE-2023-35898**	https://www.ibm.com/support/pages/node/7009205, https://exchange.xforce.ibmcloud.com/vulnerabilities/259352	A-IBM-INFO-020823/210
N/A	17-Jul-2023	5.3	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain system information using a specially crafted query that could aid in further attacks against the system. IBM X-Force ID: 257695. **CVE ID : CVE-2023-33857**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257695, https://www.ibm.com/support/pages/node/7007059	A-IBM-INFO-020823/211
Product: mq					
Affected Version(s): 9.0.0.0					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations,	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/s	A-IBM-MQ-020823/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	upport/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	
Affected Version(s): 9.1.0.0					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	A-IBM-MQ-020823/213
Affected Version(s): 9.2.0					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabi	A-IBM-MQ-020823/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lities/250397	
Affected Version(s): 9.3.0					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	A-IBM-MQ-020823/215
Product: mq_appliance					
Affected Version(s): 9.2.0.0					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	A-IBM-MQ_A-020823/216
Affected Version(s): 9.3.0.0					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2	https://www.ibm.com/support/pages/node/700	A-IBM-MQ_A-020823/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	7731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	
Product: robotic_process_automation					
Affected Version(s): * Up to (including) 21.0.7.4					
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368, https://www.ibm.com/support/pages/node/7010895	A-IBM-ROBO-020823/218
Affected Version(s): From (including) 21.0.0 Up to (including) 21.0.7.6					
Improper Authentication	17-Jul-2023	5.3	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380.	https://exchange.xforce.ibmcloud.com/vulnerabilities/259380, https://www.ibm.com/support/pages/node/7012317	A-IBM-ROBO-020823/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35901		
Affected Version(s): From (including) 23.0.0 Up to (including) 23.0.5					
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368, https://www.ibm.com/support/pages/node/7010895	A-IBM-ROBO-020823/220
Affected Version(s): From (including) 23.0.0 Up to (including) 23.0.6					
Improper Authentication	17-Jul-2023	5.3	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380. **CVE ID : CVE-2023-35901**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259380, https://www.ibm.com/support/pages/node/7012317	A-IBM-ROBO-020823/221
Product: robotic_process_automation_as_a_service					
Affected Version(s): * Up to (including) 21.0.7.4					
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368,	A-IBM-ROBO-020823/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	https://www.ibm.com/support/pages/node/7010895	
Affected Version(s): From (including) 21.0.0 Up to (including) 21.0.7.6					
Improper Authentication	17-Jul-2023	5.3	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380. **CVE ID : CVE-2023-35901**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259380, https://www.ibm.com/support/pages/node/7012317	A-IBM-ROBO-020823/223
Affected Version(s): From (including) 23.0.0 Up to (including) 23.0.5					
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368, https://www.ibm.com/support/pages/node/7010895	A-IBM-ROBO-020823/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: robotic_process_automation_for_cloud_pak					
Affected Version(s): * Up to (including) 21.0.7.4					
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368, https://www.ibm.com/support/pages/node/7010895	A-IBM-ROBO-020823/225
Affected Version(s): From (including) 21.0.0 Up to (including) 21.0.7.6					
Improper Authentication	17-Jul-2023	5.3	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380. **CVE ID : CVE-2023-35901**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259380, https://www.ibm.com/support/pages/node/7012317	A-IBM-ROBO-020823/226
Affected Version(s): From (including) 23.0.0 Up to (including) 23.0.5					
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368, https://www.ibm.com/s	A-IBM-ROBO-020823/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	upport/pages/node/7010895	
Affected Version(s): From (including) 23.0.0 Up to (including) 23.0.6					
Improper Authentication	17-Jul-2023	5.3	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380. **CVE ID : CVE-2023-35901**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259380, https://www.ibm.com/support/pages/node/7012317	A-IBM-ROBO-020823/228
Product: security_verify_access					
Affected Version(s): 10.0.0					
URL Redirection to Untrusted Site ('Open Redirect')	19-Jul-2023	5.4	IBM Security Verify Access 10.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to	https://exchange.xforce.ibmcloud.com/vulnerabilities/252186, https://www.ibm.com/support/pages/node/7012613	A-IBM-SECU-020823/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 252186. **CVE ID : CVE-2023-30433**		
Product: spectrum_protect_client					
Affected Version(s): From (including) 8.1.0.0 Up to (including) 8.1.17.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Jul-2023	4.7	IBM Spectrum Protect 8.1.0.0 through 8.1.17.0 could allow a local user to cause a denial of service due to due to improper time-of-check to time-of-use functionality. IBM X-Force ID: 256012. **CVE ID : CVE-2023-33832**	https://exchange.xforce.ibmcloud.com/vulnerabilities/256012, https://www.ibm.com/support/pages/node/7011761	A-IBM-SPEC-020823/230
Product: spectrum_protect_for_space_management					
Affected Version(s): From (including) 8.1.0.0 Up to (including) 8.1.17.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Jul-2023	4.7	IBM Spectrum Protect 8.1.0.0 through 8.1.17.0 could allow a local user to cause a denial of service due to due to improper time-of-check to time-of-use functionality. IBM X-Force ID: 256012. **CVE ID : CVE-2023-33832**	https://exchange.xforce.ibmcloud.com/vulnerabilities/256012, https://www.ibm.com/support/pages/node/7011761	A-IBM-SPEC-020823/231
Product: spectrum_protect_for_virtual_environments					
Affected Version(s): From (including) 8.1.0.0 Up to (including) 8.1.17.0					
Time-of-check	19-Jul-2023	4.7	IBM Spectrum Protect 8.1.0.0 through	https://exchange.xforce.i	A-IBM-SPEC-020823/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-use (TOCTOU) Race Condition			8.1.17.0 could allow a local user to cause a denial of service due to due to improper time-of-check to time-of-use functionality. IBM X-Force ID: 256012. **CVE ID : CVE-2023-33832**	bmcloud.com/vulnerabilities/256012, https://www.ibm.com/support/pages/node/7011761	
Product: sterling_connect					
Affected Version(s): express_for_unix					
Server-Side Request Forgery (SSRF)	19-Jul-2023	5.4	IBM Sterling Connect:Express for UNIX 1.5 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: 252135. **CVE ID : CVE-2023-29260**	https://www.ibm.com/support/pages/node/7010923, https://exchange.xforce.ibmcloud.com/vulnerabilities/252135	A-IBM-STER-020823/233
N/A	19-Jul-2023	5.3	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055. **CVE ID : CVE-2023-29259**	https://exchange.xforce.ibmcloud.com/vulnerabilities/252055, https://www.ibm.com/support/pages/node/7010921	A-IBM-STER-020823/234
Vendor: ibos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ibos					
Affected Version(s): 4.5.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jul-2023	9.8	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. Affected by this issue is the function actionExport of the file ?r=contact/default/export of the component Personal Office Address Book. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-235058 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3791**	N/A	A-IBO-IBOS-020823/235
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jul-2023	9.8	A vulnerability was found in IBOS OA 4.5.5 and classified as critical. This issue affects some unknown processing of the file ?r=article/category/del of the component Delete Category Handler. The manipulation leads to sql injection. The attack may be	N/A	A-IBO-IBOS-020823/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235067. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3799**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Jul-2023	9.8	A vulnerability has been found in IBOS OA 4.5.5 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /?r=recruit/resume/edit&op=status of the component Interview Handler. The manipulation of the argument resumeid 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-235147. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3826**	N/A	A-IBO-IBOS-020823/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Icewarp					
Product: icewarp					
Affected Version(s): 10.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	6.1	Icewarp Icearp v10.2.1 was discovered to contain a cross-site scripting (XSS) vulnerability via the color parameter. **CVE ID : CVE-2023-37728**	N/A	A-ICE-ICEW-020823/238
Vendor: icewhale					
Product: casaos-gateway					
Affected Version(s): * Up to (excluding) 0.4.4					
Missing Authentication for Critical Function	17-Jul-2023	9.8	CasaOS is an open-source Personal Cloud system. Due to a lack of IP address verification an unauthenticated attackers can execute arbitrary commands as `root` on CasaOS instances. The problem was addressed by improving the detection of client IP addresses in `391dd7f`. This patch is part of CasaOS 0.4.4. Users should upgrade to CasaOS 0.4.4. If they can't, they should temporarily restrict access to CasaOS to untrusted users, for instance by not exposing it publicly.	https://github.com/IceWhaleTech/CasaOS-Gateway/security/advisories/GHSA-vjh7-5r6x-xh6g, https://github.com/IceWhaleTech/CasaOS-Gateway/commit/391dd7f0f239020c46bf057cfa25f82031fc15f7	A-ICE-CASA-020823/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37265		
Affected Version(s): 0.4.4					
Missing Authentication for Critical Function	17-Jul-2023	9.8	CasaOS is an open-source Personal Cloud system. Due to a lack of IP address verification an unauthenticated attackers can execute arbitrary commands as `root` on CasaOS instances. The problem was addressed by improving the detection of client IP addresses in `391dd7f`. This patch is part of CasaOS 0.4.4. Users should upgrade to CasaOS 0.4.4. If they can't, they should temporarily restrict access to CasaOS to untrusted users, for instance by not exposing it publicly. **CVE ID : CVE-2023-37265**	https://github.com/IceWhaleTech/CasaOS-Gateway/security/advisories/GHSA-vjh7-5r6x-xh6g, https://github.com/IceWhaleTech/CasaOS-Gateway/commit/391dd7f0f239020c46bf057cfa25f82031fc15f7	A-ICE-CASA-020823/240
Vendor: ideastocode					
Product: enable_svg\,_webp_\&_ico_upload					
Affected Version(s): * Up to (including) 1.0.3					
Improper Neutralization of Input During Web Page Generation	17-Jul-2023	5.4	The Enable SVG, WebP & ICO Upload WordPress plugin through 1.0.3 does not sanitize SVG file contents, leading to a Cross-Site Scripting vulnerability.	N/A	A-IDE-ENAB-020823/241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-2143**		
Vendor: inactive_user_deleter_project					
Product: inactive_user_deleter					
Affected Version(s): * Up to (excluding) 1.60					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Korol Yuriy aka Shra Inactive User Deleter plugin <= 1.59 versions. **CVE ID : CVE-2023-27424**	N/A	A-INA-INAC-020823/242
Vendor: infodoc					
Product: document_on-line_submission_and_approval_system					
Affected Version(s): 22547					
Unrestricted Upload of File with Dangerous Type	20-Jul-2023	9.8	It is identified a vulnerability of Unrestricted Upload of File with Dangerous Type in the file uploading function in InfoDoc Document On-line Submission and Approval System, which allows an unauthenticated remote attacker can exploit this vulnerability without logging system to upload and run arbitrary executable files to perform arbitrary system commands or disrupt service. This issue affects Document On-line Submission and	N/A	A-INF-DOCU-020823/243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Approval System: 22547, 22567. **CVE ID : CVE-2023-37289**		
Server-Side Request Forgery (SSRF)	20-Jul-2023	7.5	InfoDoc Document On-line Submission and Approval System lacks sufficient restrictions on the available tags within its HTML to PDF conversion function, and allowing an unauthenticated attackers to load remote or local resources through HTML tags such as iframe. This vulnerability allows unauthenticated remote attackers to perform Server-Side Request Forgery (SSRF) attacks, gaining unauthorized access to arbitrary system files and uncovering the internal network topology. **CVE ID : CVE-2023-37290**	N/A	A-INF-DOCU-020823/244
Affected Version(s): 22567					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	20-Jul-2023	9.8	It is identified a vulnerability of Unrestricted Upload of File with Dangerous Type in the file uploading function in InfoDoc Document On-line Submission and Approval System, which allows an unauthenticated remote attacker can exploit this vulnerability without logging system to upload and run arbitrary executable files to perform arbitrary system commands or disrupt service. This issue affects Document On-line Submission and Approval System: 22547, 22567. **CVE ID : CVE-2023-37289**	N/A	A-INF-DOCU-020823/245
Server-Side Request Forgery (SSRF)	20-Jul-2023	7.5	InfoDoc Document On-line Submission and Approval System lacks sufficient restrictions on the available tags within its HTML to PDF conversion function, and allowing an unauthenticated attackers to load remote or local resources through HTML tags such as iframe. This	N/A	A-INF-DOCU-020823/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated remote attackers to perform Server-Side Request Forgery (SSRF) attacks, gaining unauthorized access to arbitrary system files and uncovering the internal network topology. **CVE ID : CVE-2023-37290**		
Vendor: Infodrom					
Product: e-invoice_approval_system					
Affected Version(s): * Up to (excluding) 20230701					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Infodrom Software E-Invoice Approval System allows SQL Injection.This issue affects E-Invoice Approval System: before v.20230701. **CVE ID : CVE-2023-35066**	N/A	A-INF-E-IN-020823/247
Vendor: intergard					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: smartgard_silver_with_matrix_keyboard					
Affected Version(s): 8.7.0					
N/A	19-Jul-2023	9.8	A vulnerability, which was classified as critical, was found in Intergard SGS 8.7.0. Affected is an unknown function. The manipulation leads to permission issues. 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-234444. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3759**	N/A	A-INT-SMAR-020823/248
Cleartext Transmission of Sensitive Information	19-Jul-2023	7.5	A vulnerability was found in Intergard SGS 8.7.0 and classified as problematic. Affected by this issue is some unknown functionality of the component Password Change Handler. The manipulation leads to cleartext transmission of sensitive information. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is	N/A	A-INT-SMAR-020823/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			known to be difficult. The exploit has been disclosed to the public and may be used. VDB-234446 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3761**		
Cleartext Storage of Sensitive Information	19-Jul-2023	7.5	A vulnerability was found in Intergard SGS 8.7.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to cleartext storage of sensitive information in memory. 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-234447. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3762**	N/A	A-INT-SMAR-020823/250
Cleartext Transmission of	19-Jul-2023	7.5	A vulnerability was found in Intergard SGS 8.7.0. It has been	N/A	A-INT-SMAR-020823/251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Sensitive Information			declared as problematic. This vulnerability affects unknown code of the component SQL Query Handler. The manipulation leads to cleartext transmission of sensitive information. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-234448. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3763**		
Improper Resource Shutdown or Release	19-Jul-2023	6.5	A vulnerability has been found in Intergard SGS 8.7.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Change Password Handler. The manipulation leads to denial of service. The attack can be launched remotely. The exploit has been	N/A	A-INT-SMAR-020823/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosed to the public and may be used. The identifier VDB-234445 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3760**		
Vendor: inventorypress_project					
Product: inventorypress					
Affected Version(s): * Up to (including) 1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	5.4	The InventoryPress WordPress plugin through 1.7 does not sanitise and escape some of its settings, which could allow users with the role of author and above to perform Stored Cross-Site Scripting attacks. **CVE ID : CVE-2023-2579**	N/A	A-INV-INVE-020823/253
Vendor: istrong					
Product: four_mountain_torrent_disaster_prevention\,_control_monitoring_and_early_warning_system					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	20-Jul-2023	8.8	A vulnerability, which was classified as critical, was found in Gen Technology Four Mountain Torrent Disaster Prevention and Control of Monitoring and Early Warning System up to	N/A	A-IST-FOUR-020823/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20230712. This affects an unknown part of the file /Duty/AjaxHandle/UploadFloodPlanFileUpdate.ashx. The manipulation of the argument Filedata leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The identifier VDB-235065 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3797**		
Vendor: ivanti					
Product: endpoint_manager					
Affected Version(s): * Up to (excluding) 7.9.1.285					
Out-of-bounds Write	21-Jul-2023	7.5	An out-of-bounds write vulnerability on windows operating systems causes the Ivanti AntiVirus Product to crash. Update to Ivanti AV Product version 7.9.1.285 or above. **CVE ID : CVE-2023-35077**	https://forums.ivanti.com/s/article/SA-2023-07-19-CVE-2023-35077	A-IVA-ENDP-020823/255
Vendor: jaegertracing					
Product: jaeger_ui					
Affected Version(s): * Up to (excluding) 1.31.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	5.4	Cross Site Scripting (XSS) vulnerability in Jaegertracing Jaeger UI before v.1.31.0 allows a remote attacker to execute arbitrary code via the KeyValuesTable component. **CVE ID : CVE-2023-36656**	https://github.com/mafintosh/json-markup/pull/15, https://github.com/jaegertracing/jaeger-ui/security/advisories/GHSA-vv24-rm95-q56r, https://github.com/jaegertracing/jaeger-ui/pull/1498	A-JAE-JAEG-020823/256
Vendor: Jenkins					
Product: gitlab_authentication					
Affected Version(s): * Up to (including) 1.17.1					
Cross-Site Request Forgery (CSRF)	26-Jul-2023	5.4	A cross-site request forgery (CSRF) vulnerability in Jenkins GitLab Authentication Plugin 1.17.1 and earlier allows attackers to trick users into logging in to the attacker's account. **CVE ID : CVE-2023-39153**	https://www.jenkins.io/security/advisory/2023-07-26/#SECURITY-2696	A-JEN-GITL-020823/257
Product: gradle					
Affected Version(s): 2.8					
Always-Incorrect Control Flow	26-Jul-2023	6.5	Always-incorrect control flow implementation in Jenkins Gradle Plugin 2.8 may result in	https://www.jenkins.io/security/advisory/2023-07-	A-JEN-GRAD-020823/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Implementation			credentials not being masked (i.e., replaced with asterisks) in the build log in some circumstances. **CVE ID : CVE-2023-39152**	26/#SECURITY-3208	
Product: qualys_web_app_scanning_connector					
Affected Version(s): * Up to (including) 2.0.10					
Incorrect Authorization	26-Jul-2023	6.5	Incorrect permission checks in Jenkins Qualys Web App Scanning Connector Plugin 2.0.10 and earlier allow attackers with global Item/Configure permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2023-39154**	https://www.jenkins.io/security/advisory/2023-07-26/#SECURITY-3012	A-JEN-QUAL-020823/259
Vendor: Jetbrains					
Product: teamcity					
Affected Version(s): * Up to (excluding) 2023.05.2					
Incorrect Privilege Assignment	25-Jul-2023	8.8	In JetBrains TeamCity before 2023.05.2 a token with limited permissions could be used to gain full account access **CVE ID : CVE-2023-39173**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-020823/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	25-Jul-2023	7.5	In JetBrains TeamCity before 2023.05.2 a ReDoS attack was possible via integration with issue trackers **CVE ID : CVE-2023-39174**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-020823/261
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	In JetBrains TeamCity before 2023.05.2 reflected XSS via GitHub integration was possible **CVE ID : CVE-2023-39175**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-TEAM-020823/262
Vendor: keetrax					
Product: wp_tiles					
Affected Version(s): * Up to (including) 1.1.2					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Mike Martel WP Tiles plugin <= 1.1.2 versions. **CVE ID : CVE-2023-25482**	N/A	A-KEE-WP_T-020823/263
Vendor: keylime					
Product: keylime					
Affected Version(s): * Up to (excluding) 7.2.5					
N/A	19-Jul-2023	2.8	A flaw was found in the keylime attestation verifier, which fails to flag a device's submitted TPM quote as faulty when the quote's signature does not validate for some	https://bugzilla.redhat.com/show_bug.cgi?id=2222903, https://github.com/keylime/keylime/commit/95	A-KEY-KEYL-020823/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reason. Instead, it will only emit an error in the log without flagging the device as untrusted. **CVE ID : CVE-2023-3674**	ce3d86bd2c53009108ffda2dcf553312d733db	
Vendor: keysight					
Product: geolocation_server					
Affected Version(s): * Up to (including) 2.4.2					
Unrestricted Upload of File with Dangerous Type	19-Jul-2023	7.8	In Keysight Geolocation Server v2.4.2 and prior, an attacker could upload a specially crafted malicious file or delete any file or directory with SYSTEM privileges due to an improper path validation, which could result in local privilege escalation or a denial-of-service condition.	N/A	A-KEY-GEOL-020823/265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34394		
Uncontrolled Search Path Element	19-Jul-2023	7.8	?In Keysight Geolocation Server v2.4.2 and prior, a low privileged attacker could create a local ZIP file containing a malicious script in any location. The attacker could abuse this to load a DLL with SYSTEM privileges.	N/A	A-KEY-GEOL-020823/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36853		
Vendor: layui					
Product: layui					
Affected Version(s): * Up to (excluding) 2.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in layui up to v2.8.0-rc.16. This affects an unknown part of the component HTML Attribute Handler. The manipulation of the argument title leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 2.8.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-234237 was assigned to this vulnerability. **CVE ID : CVE-2023-3691**	N/A	A-LAY-LAYU-020823/267
Affected Version(s): 2.8.0					
Improper Neutralization of Input During Web Page Generation	16-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in layui up to v2.8.0-rc.16. This affects an unknown part of the component HTML Attribute	N/A	A-LAY-LAYU-020823/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Handler. The manipulation of the argument title leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 2.8.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-234237 was assigned to this vulnerability. **CVE ID : CVE-2023-3691**		
Vendor: leothemes					
Product: ap_page_builder					
Affected Version(s): * Up to (excluding) 1.7.8.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jul-2023	7.5	Ap Page Builder, in versions lower than 1.7.8.2, could allow a remote attacker to send a specially crafted SQL query to the product_one_img parameter to retrieve the information stored in the database. **CVE ID : CVE-2023-3743**	N/A	A-LEO-AP_P-020823/269
Vendor: lfprojects					
Product: mlflow					
Affected Version(s): * Up to (excluding) 2.5.0					
Absolute Path Traversal	19-Jul-2023	10	Absolute Path Traversal in GitHub repository	https://github.com/mlflow/mlflow/commit/6dde	A-LFP-MLFL-020823/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mlflow/mlflow prior to 2.5.0. **CVE ID : CVE-2023-3765**	93758d42455cb90ef324407919ed67668b9b, https://huntr.dev/bounties/4be5fd63-8a0a-490d-9ee1-f33dc768ed76	
Vendor: life_insurance_management_system_project					
Product: life_insurance_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-2023	9.8	A vulnerability classified as critical was found in SourceCodester Life Insurance Management System 1.0. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-234244. **CVE ID : CVE-2023-3693**	N/A	A-LIF-LIFE-020823/271
Vendor: Linuxfoundation					
Product: dapr					
Affected Version(s): * Up to (excluding) 1.10.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	21-Jul-2023	7.5	Dapr is a portable, event-driven, runtime for building distributed applications across cloud and edge. A vulnerability has been found in Dapr that allows bypassing API token authentication, which is used by the Dapr sidecar to authenticate calls coming from the application, with a well-crafted HTTP request. Users who leverage API token authentication are encouraged to upgrade Dapr to 1.10.9 or to 1.11.2. This vulnerability impacts Dapr users who have configured API token authentication. An attacker could craft a request that is always allowed by the Dapr sidecar over HTTP, even if the `dapr-api-token` in the request is invalid or missing. The issue has been fixed in Dapr 1.10.9 or to 1.11.2. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37918**	https://github.com/dapr/dapr/security/advisories/GHSA-59m6-82qm-vqgj, https://github.com/dapr/dapr/commit/83ca1abb11ffe34211db55dcd36d96b94252827a	A-LIN-DAPR-020823/272
Affected Version(s): From (including) 1.11.0 Up to (excluding) 1.11.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	21-Jul-2023	7.5	Dapr is a portable, event-driven, runtime for building distributed applications across cloud and edge. A vulnerability has been found in Dapr that allows bypassing API token authentication, which is used by the Dapr sidecar to authenticate calls coming from the application, with a well-crafted HTTP request. Users who leverage API token authentication are encouraged to upgrade Dapr to 1.10.9 or to 1.11.2. This vulnerability impacts Dapr users who have configured API token authentication. An attacker could craft a request that is always allowed by the Dapr sidecar over HTTP, even if the `dapr-api-token` in the request is invalid or missing. The issue has been fixed in Dapr 1.10.9 or to 1.11.2. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37918**	https://github.com/dapr/dapr/security/advisories/GHSA-59m6-82qm-vqgj, https://github.com/dapr/dapr/commit/83ca1abb11ffe34211db55dcd36d96b94252827a	A-LIN-DAPR-020823/273
Vendor: liquidweb					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: restrict_content					
Affected Version(s): * Up to (excluding) 3.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	The Membership WordPress plugin before 3.2.3 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin **CVE ID : CVE-2023-3182**	N/A	A-LIQ-REST-020823/274
Vendor: livelyworks					
Product: articart					
Affected Version(s): 2.0.1					
URL Redirection to Untrusted Site ('Open Redirect')	16-Jul-2023	6.1	A vulnerability was found in LivelyWorks Articart 2.0.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /change-language/de_DE of the component Base64 Encoding Handler. The manipulation of the argument redirectTo leads to open redirect. The attack may be launched remotely. VDB-234230 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure	N/A	A-LIV-ARTI-020823/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			but did not respond in any way. **CVE ID : CVE-2023-3684**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-2023	5.4	A vulnerability has been found in LivelyWorks Articart 2.0.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /items/search. The manipulation of the argument search_term leads to cross site scripting. The attack can be launched remotely. The identifier VDB-234229 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3683**	N/A	A-LIV-ARTI-020823/276
Vendor: login_configurator_project					
Product: login_configurator					
Affected Version(s): * Up to (including) 2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	The Login Configurator WordPress plugin through 2.1 does not properly escape a URL parameter before outputting it to the page, leading to a reflected cross-site scripting vulnerability	N/A	A-LOG-LOGI-020823/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			targeting site administrators. **CVE ID : CVE-2023-1893**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in GrandSlambert Login Configurator plugin <= 2.1 versions. **CVE ID : CVE-2023-34369**	N/A	A-LOG-LOGI-020823/278
Vendor: lost_and_found_information_system_project					
Product: lost_and_found_information_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jul-2023	9.8	A vulnerability has been found in SourceCodester Lost and Found Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=delete_category of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-235201 was assigned to this vulnerability. **CVE ID : CVE-2023-3850**	N/A	A-LOS-LOST-020823/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: mage-people					
Product: event_manager_and_tickets_selling_for_woocommerce					
Affected Version(s): * Up to (including) 3.9.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	5.4	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in MagePeople Team Event Manager and Tickets Selling Plugin for WooCommerce plugin <= 3.9.5 versions. **CVE ID : CVE-2023-36383**	N/A	A-MAG-EVEN-020823/280
Vendor: mainwp					
Product: mainwp_maintenance_extension					
Affected Version(s): * Up to (including) 4.1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jul-2023	8.8	Auth. (subscriber+) SQL Injection (SQLi) vulnerability in MainWP MainWP Maintenance Extension plugin <= 4.1.1 versions. **CVE ID : CVE-2023-23660**	N/A	A-MAI-MAIN-020823/281
Vendor: matrix-react-sdk_project					
Product: matrix-react-sdk					
Affected Version(s): 3.76.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	5.4	matrix-react-sdk is a react-based SDK for inserting a Matrix chat/voip client into a web page. The Export Chat feature includes certain attacker-controlled elements in the generated document without	https://github.com/matrix-org/matrix-react-sdk/commit/22fcd34c606f32129ebc9	A-MAT-MATR-020823/282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sufficient escaping, leading to stored Cross site scripting (XSS). Since the Export Chat feature generates a separate document, an attacker can only inject code run from the `null` origin, restricting the impact. However, the attacker can still potentially use the XSS to leak message contents. A malicious homeserver is a potential attacker since the affected inputs are controllable server-side. This issue has been addressed in commit `22fcd34c60` which is included in release version 3.76.0. Users are advised to upgrade. The only known workaround for this issue is to disable or to not use the Export Chat feature. **CVE ID : CVE-2023-37259**	67fc21f24fb708a98b8	
Affected Version(s): From (including) 3.32.0 Up to (excluding) 3.76.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	5.4	matrix-react-sdk is a react-based SDK for inserting a Matrix chat/voip client into a web page. The Export Chat feature includes certain attacker-controlled elements in the generated document without	https://github.com/matrix-org/matrix-react-sdk/commit/22fcd34c606f32129ebc967fc21f24fb708a98b8	A-MAT-MATR-020823/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sufficient escaping, leading to stored Cross site scripting (XSS). Since the Export Chat feature generates a separate document, an attacker can only inject code run from the `null` origin, restricting the impact. However, the attacker can still potentially use the XSS to leak message contents. A malicious homeserver is a potential attacker since the affected inputs are controllable server-side. This issue has been addressed in commit `22fcd34c60` which is included in release version 3.76.0. Users are advised to upgrade. The only known workaround for this issue is to disable or to not use the Export Chat feature. **CVE ID : CVE-2023-37259**		
Vendor: mattermost					
Product: mattermost					
Affected Version(s): * Up to (excluding) 2.5.1					
Improper Certificate Validation	17-Jul-2023	8.1	Mattermost iOS app fails to properly validate the server certificate while initializing the TLS connection allowing a network	https://mattermost.com/security-updates	A-MAT-MATT-020823/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to intercept the WebSockets connection. **CVE ID : CVE-2023-3615**		
Product: mattermost_server					
Affected Version(s): * Up to (excluding) 7.8.6					
Incorrect Authorization	17-Jul-2023	3.5	Mattermost WelcomeBot plugin fails to to validate the membership status when inviting or adding users to channels allowing guest accounts to be added or invited to channels by default. **CVE ID : CVE-2023-3613**	https://mattermost.com/security-updates	A-MAT-MATT-020823/285
Affected Version(s): * Up to (excluding) 7.8.7					
Uncontrolled Resource Consumption	17-Jul-2023	4.3	Mattermost Boards fail to properly validate a board link, allowing an attacker to crash a channel by posting a specially crafted boards link. **CVE ID : CVE-2023-3585**	https://mattermost.com/security-updates	A-MAT-MATT-020823/286
Uncontrolled Resource Consumption	17-Jul-2023	3.3	Mattermost fails to properly validate a gif image file, allowing an attacker to consume a significant amount of server resources, making the server unresponsive for an extended period of time by linking to	https://mattermost.com/security-updates	A-MAT-MATT-020823/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specially crafted image file. **CVE ID : CVE-2023-3614**		
Affected Version(s): From (including) 7.10.0 Up to (excluding) 7.10.3					
Improper Authentication	17-Jul-2023	8.2	Mattermost fails to invalidate previously generated password reset tokens when a new reset token was created. **CVE ID : CVE-2023-3591**	https://mattermost.com/security-updates	A-MAT-MATT-020823/288
Origin Validation Error	17-Jul-2023	8.1	Mattermost fails to properly validate the origin of a websocket connection allowing a MITM attacker on Mattermost to access the websocket APIs. **CVE ID : CVE-2023-3581**	https://mattermost.com/security-updates	A-MAT-MATT-020823/289
Incorrect Authorization	17-Jul-2023	7.5	Mattermost fails to delete card attachments in Boards, allowing an attacker to access deleted attachments. **CVE ID : CVE-2023-3590**	https://mattermost.com/security-updates	A-MAT-MATT-020823/290
N/A	17-Jul-2023	6.5	Mattermost fails to properly validate markdown, allowing an attacker to crash the server via a specially crafted markdown input. **CVE ID : CVE-2023-3593**	https://mattermost.com/security-updates	A-MAT-MATT-020823/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-Jul-2023	5.4	Mattermost fails to disable public Boards after the "Enable Publicly-Shared Boards" configuration option is disabled, resulting in previously-shared public Boards to remain accessible. **CVE ID : CVE-2023-3586**	https://mattermost.com/security-updates	A-MAT-MATT-020823/292
Server-Side Request Forgery (SSRF)	17-Jul-2023	4.3	Mattermost fails to properly restrict requests to localhost/intranet during the interactive dialog, which could allow an attacker to perform a limited blind SSRF. **CVE ID : CVE-2023-3577**	https://mattermost.com/security-updates	A-MAT-MATT-020823/293
Incorrect Authorization	17-Jul-2023	4.3	Mattermost fails to verify channel membership when linking a board to a channel allowing a low-privileged authenticated user to link a Board to a private channel they don't have access to, **CVE ID : CVE-2023-3582**	https://mattermost.com/security-updates	A-MAT-MATT-020823/294
Uncontrolled Resource Consumption	17-Jul-2023	4.3	Mattermost Boards fail to properly validate a board link, allowing an attacker to crash a channel by posting a specially crafted boards link.	https://mattermost.com/security-updates	A-MAT-MATT-020823/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3585		
Uncontrolled Resource Consumption	17-Jul-2023	3.3	Mattermost fails to properly validate a gif image file, allowing an attacker to consume a significant amount of server resources, making the server unresponsive for an extended period of time by linking to specially crafted image file. **CVE ID : CVE-2023-3614**	https://mattermost.com/security-updates	A-MAT-MATT-020823/296
Incorrect Authorization	17-Jul-2023	3.1	Mattermost fails to properly check the authorization of POST /api/v4/teams when passing a team override scheme ID in the request, allowing an authenticated attacker with knowledge of a Team Override Scheme ID to create a new team with said team override scheme. **CVE ID : CVE-2023-3584**	https://mattermost.com/security-updates	A-MAT-MATT-020823/297
Missing Authorization	17-Jul-2023	2.7	Mattermost fails to properly show information in the UI, allowing a system admin to modify a board state allowing any user with a valid sharing link to join the board with editor access, without the UI	https://mattermost.com/security-updates	A-MAT-MATT-020823/298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			showing the updated permissions. **CVE ID : CVE-2023-3587**		
Affected Version(s): From (including) 7.8.0 Up to (excluding) 7.8.5					
Incorrect Authorization	17-Jul-2023	3.1	Mattermost fails to properly check the authorization of POST /api/v4/teams when passing a team override scheme ID in the request, allowing an authenticated attacker with knowledge of a Team Override Scheme ID to create a new team with said team override scheme. **CVE ID : CVE-2023-3584**	https://mattermost.com/security-updates	A-MAT-MATT-020823/299
Affected Version(s): From (including) 7.8.0 Up to (excluding) 7.8.7					
Improper Authentication	17-Jul-2023	8.2	Mattermost fails to invalidate previously generated password reset tokens when a new reset token was created. **CVE ID : CVE-2023-3591**	https://mattermost.com/security-updates	A-MAT-MATT-020823/300
Origin Validation Error	17-Jul-2023	8.1	Mattermost fails to properly validate the origin of a websocket connection allowing a MITM attacker on Mattermost to access the websocket APIs. **CVE ID : CVE-2023-3581**	https://mattermost.com/security-updates	A-MAT-MATT-020823/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Jul-2023	6.5	Mattermost fails to properly validate markdown, allowing an attacker to crash the server via a specially crafted markdown input. **CVE ID : CVE-2023-3593**	https://mattermost.com/security-updates	A-MAT-MATT-020823/302
Incorrect Authorization	17-Jul-2023	5.4	Mattermost fails to disable public Boards after the "Enable Publicly-Shared Boards" configuration option is disabled, resulting in previously-shared public Boards to remain accessible. **CVE ID : CVE-2023-3586**	https://mattermost.com/security-updates	A-MAT-MATT-020823/303
Server-Side Request Forgery (SSRF)	17-Jul-2023	4.3	Mattermost fails to properly restrict requests to localhost/intranet during the interactive dialog, which could allow an attacker to perform a limited blind SSRF. **CVE ID : CVE-2023-3577**	https://mattermost.com/security-updates	A-MAT-MATT-020823/304
Incorrect Authorization	17-Jul-2023	4.3	Mattermost fails to verify channel membership when linking a board to a channel allowing a low-privileged authenticated user to link a Board to a	https://mattermost.com/security-updates	A-MAT-MATT-020823/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			private channel they don't have access to, **CVE ID : CVE-2023-3582**		
Missing Authorization	17-Jul-2023	2.7	Mattermost fails to properly show information in the UI, allowing a system admin to modify a board state allowing any user with a valid sharing link to join the board with editor access, without the UI showing the updated permissions. **CVE ID : CVE-2023-3587**	https://mattermost.com/security-updates	A-MAT-MATT-020823/306
Affected Version(s): From (including) 7.9.0 Up to (excluding) 7.10.3					
Incorrect Authorization	17-Jul-2023	3.5	Mattermost WelcomeBot plugin fails to to validate the membership status when inviting or adding users to channels allowing guest accounts to be added or invited to channels by default. **CVE ID : CVE-2023-3613**	https://mattermost.com/security-updates	A-MAT-MATT-020823/307
Affected Version(s): From (including) 7.9.0 Up to (excluding) 7.9.5					
Improper Authentication	17-Jul-2023	8.2	Mattermost fails to invalidate previously generated password reset tokens when a new reset token was created. **CVE ID : CVE-2023-3591**	https://mattermost.com/security-updates	A-MAT-MATT-020823/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	17-Jul-2023	8.1	Mattermost fails to properly validate the origin of a websocket connection allowing a MITM attacker on Mattermost to access the websocket APIs. **CVE ID : CVE-2023-3581**	https://mattermost.com/security-updates	A-MAT-MATT-020823/309
N/A	17-Jul-2023	6.5	Mattermost fails to properly validate markdown, allowing an attacker to crash the server via a specially crafted markdown input. **CVE ID : CVE-2023-3593**	https://mattermost.com/security-updates	A-MAT-MATT-020823/310
Incorrect Authorization	17-Jul-2023	5.4	Mattermost fails to disable public Boards after the "Enable Publicly-Shared Boards" configuration option is disabled, resulting in previously-shared public Boards to remain accessible. **CVE ID : CVE-2023-3586**	https://mattermost.com/security-updates	A-MAT-MATT-020823/311
Incorrect Authorization	17-Jul-2023	4.3	Mattermost fails to verify channel membership when linking a board to a channel allowing a low-privileged authenticated user to link a Board to a private channel they don't have access to,	https://mattermost.com/security-updates	A-MAT-MATT-020823/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3582		
Uncontrolled Resource Consumption	17-Jul-2023	4.3	Mattermost Boards fail to properly validate a board link, allowing an attacker to crash a channel by posting a specially crafted boards link. **CVE ID : CVE-2023-3585**	https://mattermost.com/security-updates	A-MAT-MATT-020823/313
Uncontrolled Resource Consumption	17-Jul-2023	3.3	Mattermost fails to properly validate a gif image file, allowing an attacker to consume a significant amount of server resources, making the server unresponsive for an extended period of time by linking to specially crafted image file. **CVE ID : CVE-2023-3614**	https://mattermost.com/security-updates	A-MAT-MATT-020823/314
Vendor: Maxfoundry					
Product: maxbuttons					
Affected Version(s): * Up to (including) 9.5.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	5.4	Auth. (contributor+) Cross-Site Scripting (XSS) vulnerability in Max Foundry WordPress Button Plugin MaxButtons plugin <= 9.5.3 versions. **CVE ID : CVE-2023-36503**	N/A	A-MAX-MAXB-020823/315
Vendor: mediaburst					
Product: gravity_forms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.7.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	The Gravity Forms WordPress plugin before 2.7.5 does not escape generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting which could be used against high-privileged users such as admin. **CVE ID : CVE-2023-2701**	N/A	A-MED-GRAV-020823/316
Vendor: metabase					
Product: metabase					
Affected Version(s): * Up to (excluding) 0.43.7.2					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2. **CVE ID : CVE-2023-38646**	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/317
Affected Version(s): * Up to (excluding) 1.43.7.2					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2. **CVE ID : CVE-2023-38646**		
Affected Version(s): From (including) 0.44.0 Up to (excluding) 0.44.7.1					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2. **CVE ID : CVE-2023-38646**	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/319
Affected Version(s): From (including) 0.45.0 Up to (excluding) 0.45.4.1					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2. **CVE ID : CVE-2023-38646**		
Affected Version(s): From (including) 0.46.0 Up to (excluding) 0.46.6.1					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2. **CVE ID : CVE-2023-38646**	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/321
Affected Version(s): From (including) 1.44.0 Up to (excluding) 1.44.7.1					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2.	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38646		
Affected Version(s): From (including) 1.45.0 Up to (excluding) 1.45.4.1					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2. **CVE ID : CVE-2023-38646**	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/323
Affected Version(s): From (including) 1.46.0 Up to (excluding) 1.46.6.1					
N/A	21-Jul-2023	9.8	Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2. **CVE ID : CVE-2023-38646**	https://www.metabase.com/blog/security-advisory	A-MET-META-020823/324
Vendor: metagauss					
Product: profilegrid					
Affected Version(s): * Up to (excluding) 5.5.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	18-Jul-2023	8.8	The ProfileGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'edit_group' handler in versions up to, and including, 5.5.2. This makes it possible for authenticated attackers, with group ownership, to update group options, including the 'associate_role' parameter, which defines the member's role. This issue was partially patched in version 5.5.2 preventing privilege escalation, however, it was fully patched in 5.5.3. **CVE ID : CVE-2023-3714**	https://plugins.trac.wordpress.org/browser/profilegrid-user-profiles-groups-and-communities/tags/5.4.8/public/partials/profile-magic-group.php#L80	A-MET-PROF-020823/325
Affected Version(s): * Up to (including) 5.5.1					
Missing Authorization	18-Jul-2023	8.8	The ProfileGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'profile_magic_check_smtp_connection' function in versions up to, and including, 5.5.1. This makes it	https://plugins.trac.wordpress.org/browser/profilegrid-user-profiles-groups-and-communities/tags/5.4.8/admin/class-profile-magic-admin.php#	A-MET-PROF-020823/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible for authenticated attackers, with subscriber-level permissions or above to update the site options arbitrarily. This can be used by attackers to achieve privilege escalation. **CVE ID : CVE-2023-3713**	L599, https://plugins.trac.wordpress.org/changeset/2938904/profilegrid-user-profiles-groups-and-communities#file0	
Missing Authorization	18-Jul-2023	4.3	The ProfileGrid plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'pm_upload_csv' function in versions up to, and including, 5.5.1. This makes it possible for authenticated attackers, with subscriber-level permissions or above to import new users and update existing users. **CVE ID : CVE-2023-3403**	https://plugins.trac.wordpress.org/browser/profilegrid-user-profiles-groups-and-communities/tags/5.4.8/admin/class-profile-magic-admin.php#L1027, https://plugins.trac.wordpress.org/changeset/2938904/profilegrid-user-profiles-groups-and-communities#file0	A-MET-PROF-020823/327
Vendor: metersphere					
Product: metersphere					
Affected Version(s): * Up to (excluding) 2.10.3					
Improper Limitation of a	17-Jul-2023	9.8	Metersphere is an opensource testing framework. Files	N/A	A-MET-METE-020823/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			uploaded to Metersphere may define a `belongType` value with a relative path like `../../../../` which may cause metersphere to attempt to overwrite an existing file in the defined location or to create a new file. Attackers would be limited to overwriting files that the metersphere process has access to. This issue has been addressed in version 2.10.3. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37461**		
Vendor: Microfocus					
Product: cobol_server					
Affected Version(s): 6.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server.	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-COBO-020823/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 7.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the	https://portal.microfocus.com/s/article/KM0000	A-MIC-COBO-020823/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts	19323?language=en_US	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 8.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-COBO-020823/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Product: dimensions_cm					
Affected Version(s): From (including) 0.8.17 Up to (excluding) 0.9.3.1					
N/A	19-Jul-2023	6.5	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/ **CVE ID : CVE-2023-32261**	https://portal.microfocus.com/s/article/KM000019297	A-MIC-DIME-020823/332
N/A	19-Jul-2023	6.5		https://portal.microfocu	A-MIC-DIME-020823/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability allows attackers with Item/Configure permission to access and capture credentials they are not entitled to. See the following Jenkins security advisory for details: * https://www.jenkins.io/security/advisory/2023-06-14/ https://www.jenkins.io/security/advisory/2023-06-14/ **CVE ID : CVE-2023-32262**	s.com/s/article/KM000019298	
Affected Version(s): From (including) 0.8.17 Up to (including) 0.9.3					
N/A	19-Jul-2023	5.7	A potential vulnerability has been identified in the Micro Focus Dimensions CM Plugin for Jenkins. The vulnerability could be exploited to retrieve a login certificate if an authenticated user is duped into using an attacker-controlled Dimensions CM server. This vulnerability only applies when the Jenkins plugin is configured to use	https://portal.microfocus.com/s/article/KM000019293	A-MIC-DIME-020823/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			login certificate credentials. https://www.jenkins.io/security/advisory/2023-06-14/ **CVE ID : CVE-2023-32263**		
Product: enterprise_developer					
Affected Version(s): 6.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue.	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 7.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 8.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer,	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Product: enterprise_server					
Affected Version(s): 6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 7.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue.	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 8.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Product: enterprise_test_server					
Affected Version(s): 6.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server,	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 8.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue.	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-ENTE-020823/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Product: visual_cobol					
Affected Version(s): 6.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-VISU-020823/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 7.0					
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server,	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-VISU-020823/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Affected Version(s): 8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jul-2023	6.5	A potential security vulnerability has been identified in the Enterprise Server Common Web Administration (ESCWA) component used in Enterprise Server, Enterprise Test Server, Enterprise Developer, Visual COBOL, and COBOL Server. An attacker would need to be authenticated into ESCWA to attempt to exploit this vulnerability. As described in the hardening guide in the product documentation, other mitigations including restricting network access to ESCWA and restricting usersâ€™ permissions in the Micro Focus Directory Server also reduce the exposure to this issue. Given the right conditions this vulnerability could be exploited to expose a service account password. The account corresponding to the exposed credentials usually has limited privileges and, in	https://portal.microfocus.com/s/article/KM000019323?language=en_US	A-MIC-VISU-020823/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			many cases would only be useful for extracting details of other user accounts and similar information. **CVE ID : CVE-2023-32265**		
Vendor: Microsoft					
Product: chakracore					
Affected Version(s): -					
Out-of-bounds Write	18-Jul-2023	5.5	ChakraCore branch master cbb9b was discovered to contain a stack overflow vulnerability via the function Js::ScopeSlots::IsDebuggerScopeSlotArray(). **CVE ID : CVE-2023-37139**	N/A	A-MIC-CHAK-020823/347
Uncontrolled Resource Consumption	18-Jul-2023	5.5	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::DiagScopeVariablesWalker::GetChildrenCount(). **CVE ID : CVE-2023-37140**	N/A	A-MIC-CHAK-020823/348
Uncontrolled Resource Consumption	18-Jul-2023	5.5	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::ProfilingHelpers::ProfiledNewScArray().	N/A	A-MIC-CHAK-020823/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37141		
Uncontrolled Resource Consumption	18-Jul-2023	5.5	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function Js::EntryPointInfo::HasInlinees(). **CVE ID : CVE-2023-37142**	N/A	A-MIC-CHAK-020823/350
Uncontrolled Resource Consumption	18-Jul-2023	5.5	ChakraCore branch master cbb9b was discovered to contain a segmentation violation via the function BackwardPass::IsEmptyLoopAfterMemOp(). **CVE ID : CVE-2023-37143**	https://github.com/chakra-core/ChakraCore/issues/6888	A-MIC-CHAK-020823/351
Vendor: millhouse-project_project					
Product: millhouse-project					
Affected Version(s): 1.414					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jul-2023	9.8	Millhouse-Project v1.414 was discovered to contain a remote code execution (RCE) vulnerability via the component /add_post_sql.php. **CVE ID : CVE-2023-37165**	N/A	A-MIL-MILL-020823/352
Vendor: miniupnp_project					
Product: ngiflib					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	19-Jul-2023	5.5	ngiflib commit 5e7292 was discovered to contain an infinite loop via the function DecodeGifImg at ngiflib.c. **CVE ID : CVE-2023-37748**	https://github.com/miniupnp/ngiflib/issues/25	A-MIN-NGIF-020823/353
Vendor: mobisystems					
Product: office_suite					
Affected Version(s): 10.9.1.42602					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jul-2023	7.5	Office Suite Premium v10.9.1.42602 was discovered to contain a local file inclusion (LFI) vulnerability via the component /etc/hosts. **CVE ID : CVE-2023-37601**	N/A	A-MOB-OFFI-020823/354
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	6.1	Office Suite Premium Version v10.9.1.42602 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the id parameter at /api?path=profile. **CVE ID : CVE-2023-37600**	N/A	A-MOB-OFFI-020823/355
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	6.1	Office Suite Premium Version v10.9.1.42602 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the filter parameter at /api?path=files. **CVE ID : CVE-2023-38617**	N/A	A-MOB-OFFI-020823/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: mongoosejs					
Product: mongoose					
Affected Version(s): * Up to (excluding) 7.3.4					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	17-Jul-2023	9.8	Prototype Pollution in GitHub repository automattic/mongoose prior to 7.3.4. **CVE ID : CVE-2023-3696**	https://hunter.dev/bounties/1eef5a72-f6ab-4f61-b31d-fc66f5b4b467, https://github.com/automattic/mongoose/commit/305ce4ff789261df7e3f6e72363d0703e025f80d	A-MON-MONG-020823/357
Vendor: moosocial					
Product: moodating					
Affected Version(s): 1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	6.1	A vulnerability was found in mooSocial mooDating 1.2. It has been classified as problematic. Affected is an unknown function of the file /matchmakings/question of the component URL Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. VDB-235194 is the identifier assigned to this vulnerability. NOTE: We tried to contact the vendor early about the disclosure but the	N/A	A-MOO-MOOD-020823/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			official mail address was not working properly. **CVE ID : CVE-2023-3843**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	6.1	A vulnerability was found in mooSocial mooDating 1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /friends of the component URL Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235195. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly. **CVE ID : CVE-2023-3844**	N/A	A-MOO-MOOD-020823/359
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	6.1	A vulnerability was found in mooSocial mooDating 1.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /friends/ajax_invite of the component URL Handler. The	N/A	A-MOO-MOOD-020823/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235196. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly. **CVE ID : CVE-2023-3845**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	6.1	A vulnerability classified as problematic has been found in mooSocial mooDating 1.2. This affects an unknown part of the file /pages of the component URL Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235197 was assigned to this vulnerability. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly. **CVE ID : CVE-2023-3846**	N/A	A-MOO-MOOD-020823/361
Improper Neutralization of	23-Jul-2023	6.1	A vulnerability classified as problematic was	N/A	A-MOO-MOOD-020823/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			found in mooSocial mooDating 1.2. This vulnerability affects unknown code of the file /users of the component URL Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. VDB-235198 is the identifier assigned to this vulnerability. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly. **CVE ID : CVE-2023-3847**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	6.1	A vulnerability, which was classified as problematic, has been found in mooSocial mooDating 1.2. This issue affects some unknown processing of the file /users/view of the component URL Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-235199. NOTE: We tried to contact the vendor early about the	N/A	A-MOO-MOOD-020823/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure but the official mail address was not working properly. **CVE ID : CVE-2023-3848**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in mooSocial mooDating 1.2. Affected is an unknown function of the file /find-a-match of the component URL Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-235200. NOTE: We tried to contact the vendor early about the disclosure but the official mail address was not working properly. **CVE ID : CVE-2023-3849**	N/A	A-MOO-MOOD-020823/364
Vendor: mycred					
Product: mycred					
Affected Version(s): * Up to (including) 2.5.1					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in myCred plugin <= 2.5 versions. **CVE ID : CVE-2023-35096**	N/A	A-MYC-MYCR-020823/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: ncia					
Product: advisor_network					
Affected Version(s): * Up to (including) 3.3.0					
NULL Pointer Dereference	18-Jul-2023	5.5	In NATO Communications and Information Agency anet (aka Advisor Network) through 3.3.0, an attacker can provide a crafted JSON file to sanitizeJson and cause an exception. This is related to the U+FFFD Unicode replacement character. A for loop does not consider that a data structure is being modified during loop execution. **CVE ID : CVE-2023-31441**	N/A	A-NCI-ADVI-020823/366
Vendor: nesote					
Product: inout_search_engine_ai_edition					
Affected Version(s): 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-2023	5.4	A vulnerability was found in Nesote Inout Search Engine AI Edition 1.1. It has been classified as problematic. This affects an unknown part of the file /index.php. The manipulation of the argument page leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this	N/A	A-NES-INOU-020823/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-234231. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3685**		
Vendor: netentsec					
Product: application_security_gateway					
Affected Version(s): 6.3					
Direct Request ('Forced Browsing')	20-Jul-2023	6.5	A vulnerability was found in Beijing Netcon NS-ASG 6.3. It has been classified as problematic. This affects an unknown part of the file /admin/test_status.php. The manipulation leads to direct request. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-235059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3792**	N/A	A-NET-APPL-020823/368
Vendor: nxfilter					
Product: nxfilter					
Affected Version(s): 4.3.2.5					
Cross-Site Request	23-Jul-2023	8.8	A vulnerability has been found in NxFilter 4.3.2.5 and classified as problematic. This	N/A	A-NXF-NXFI-020823/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerability affects unknown code of the file user.jsp. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The identifier of this vulnerability is VDB-235192. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3841**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in NxFilter 4.3.2.5. This affects an unknown part of the file /report,daily.jsp?stime=2023%2F07%2F12&timeOption=yesterday&. The manipulation of the argument user leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-235191. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3840**	N/A	A-NXF-NXFI-020823/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: olivaekspertiz					
Product: oliva_ekspertiz					
Affected Version(s): * Up to (excluding) 1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oliva Expertise Oliva Expertise EKS allows SQL Injection.This issue affects Oliva Expertise EKS: before 1.2. **CVE ID : CVE-2023-2963**	N/A	A-OLI-OLIV-020823/371
Improper Authentication	17-Jul-2023	7.5	Authentication Bypass by Primary Weakness vulnerability in Oliva Expertise Oliva Expertise EKS allows Collect Data as Provided by Users.This issue affects Oliva Expertise EKS: before 1.2. **CVE ID : CVE-2023-2959**	N/A	A-OLI-OLIV-020823/372
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Oliva Expertise Oliva Expertise EKS allows Cross-Site Scripting (XSS).This issue affects Oliva Expertise EKS: before 1.2.	N/A	A-OLI-OLIV-020823/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2960		
Vendor: Omnis					
Product: studio					
Affected Version(s): 10.22.00					
N/A	20-Jul-2023	6.5	Omnis Studio 10.22.00 has incorrect access control. It advertises an irreversible feature for locking classes within Omnis libraries: it should be no longer possible to delete, view, change, copy, rename, duplicate, or print a locked class. Due to implementation issues, locked classes in Omnis libraries can be unlocked, and thus further analyzed and modified by Omnis Studio. This allows for further analyzing and also deleting, viewing, changing, copying, renaming, duplicating, or printing previously locked Omnis classes. This violates the expected behavior of an "irreversible operation." **CVE ID : CVE-2023-38334**	N/A	A-OMN-STUD-020823/374
N/A	20-Jul-2023	5.3	Omnis Studio 10.22.00 has incorrect access control. It advertises a feature for making Omnis libraries "always private" - this	N/A	A-OMN-STUD-020823/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is supposed to be an irreversible operation. However, due to implementation issues, "always private" Omnis libraries can be opened by the Omnis Studio browser by bypassing specific checks. This violates the expected behavior of an "irreversible operation". **CVE ID : CVE-2023-38335**		
Vendor: Openbsd					
Product: openssh					
Affected Version(s): * Up to (excluding) 9.3					
Unquoted Search Path or Element	20-Jul-2023	9.8	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. **CVE ID : CVE-2023-38408**	https://github.com/openbsd/src/commit/7bc29a9d5cd697290aa056e94ecee6253d3425f8, https://www.openssh.com/txt/release-9.3p2, https://news.ycombinator.com/item?id=36790196, https://github.com/openbsd/src/commit/f8f5a6b003981bb824329dc987d	A-OPE-OPEN-020823/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				101977beda7ca	
Affected Version(s): 9.3					
Unquoted Search Path or Element	20-Jul-2023	9.8	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. **CVE ID : CVE-2023-38408**	https://github.com/openbsd/src/commit/7bc29a9d5cd697290aa056e94ecee6253d3425f8, https://www.openssh.com/txt/release-9.3p2, https://news.ycombinator.com/item?id=36790196, https://github.com/openbsd/src/commit/f8f5a6b003981bb824329dc987d101977beda7ca	A-OPE-OPEN-020823/377
Vendor: openenclave					
Product: openenclave					
Affected Version(s): * Up to (excluding) 0.19.3					
Improper Initialization	17-Jul-2023	7.5	Open Enclave is a hardware-agnostic open source library for developing applications that utilize Hardware-based Trusted Execution Environments, also known as Enclaves. There are two issues	https://github.com/openenclave/openenclave/commit/ca54623333875b9beaad92c999a92b015c44b079, https://github.com/opene	A-OPE-OPEN-020823/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are mitigated in version 0.19.3. First, Open Enclave SDK does not properly sanitize the `MXCSR` register on enclave entry. This makes applications vulnerable to MXCSR Configuration Dependent Timing (MCDT) attacks, where incorrect `MXCSR` values can impact instruction retirement by at most one cycle, depending on the (secret) data operand value. Please find more details in the guidance from Intel in the references. Second, Open Enclave SDK does not sanitize x86's alignment check flag `RFLAGS.AC` on enclave entry. This opens up the possibility for a side-channel attacker to be notified for every unaligned memory access performed by the enclave. The issue has been addressed in version 0.19.3 and the current master branch. Users will need to recompile their applications against the patched libraries to be protected from this vulnerability. There	nclave/openenclave/security/advisories/GHSA-5gfr-m6mx-p5w4	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are no known workarounds for this vulnerability. **CVE ID : CVE-2023-37479**		
Vendor: openidentityplatform					
Product: openam					
Affected Version(s): * Up to (excluding) 14.7.3					
Improper Authentication	20-Jul-2023	9.8	Open Access Management (OpenAM) is an access management solution that includes Authentication, SSO, Authorization, Federation, Entitlements and Web Services Security. OpenAM up to version 14.7.2 does not properly validate the signature of SAML responses received as part of the SAMLv1.x Single Sign-On process. Attackers can use this fact to impersonate any OpenAM user, including the administrator, by sending a specially crafted SAML response to the SAMLPOSTProfileServlet servlet. This problem has been patched in OpenAM 14.7.3-SNAPSHOT and later. User unable to upgrade should comment servlet	https://github.com/OpenIdentityPlatform/OpenAM/pull/624, https://github.com/OpenIdentityPlatform/OpenAM/commit/7c18543d126e8a567b83bb4535631825aaa9d742, https://github.com/OpenIdentityPlatform/OpenAM/security/advisories/GHSA-4mh8-9wq6-rjxg	A-OPE-OPEN-020823/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`SAMLPOSTProfileServlet` from their pom file. See the linked GHSA for details. **CVE ID : CVE-2023-37471**		
Vendor: openrefine					
Product: openrefine					
Affected Version(s): * Up to (including) 3.7.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-2023	7.8	OpenRefine is a free, open source tool for data processing. A carefully crafted malicious OpenRefine project tar file can be used to trigger arbitrary code execution in the context of the OpenRefine process if a user can be convinced to import it. The vulnerability exists in all versions of OpenRefine up to and including 3.7.3. Users should update to OpenRefine 3.7.4 as soon as possible. Users unable to upgrade should only import OpenRefine projects from trusted sources. **CVE ID : CVE-2023-37476**	https://github.com/OpenRefine/OpenRefine/commit/e9c1e65d58b47aec8cd676bd5c07d97b002f205e, https://github.com/OpenRefine/OpenRefine/security/advisories/GHSA-m88m-crr9-jvqq	A-OPE-OPEN-020823/380
Vendor: Openssl					
Product: openssl					
Affected Version(s): 1.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jul-2023	5.3	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fc9867c1e03c22ebf56943be205202e576aabf23, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8780a896543a654e757db1b9396383f9d8095528, https://www.openssl.org/news/secadv/20230719.txt	A-OPE-OPEN-020823/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. **CVE ID : CVE-2023-3446**		
Affected Version(s): 3.0.0					
N/A	19-Jul-2023	5.3	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p'	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fc9867c1e03c22ebf56943be205202e576aabf23, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8780a896543a654e757db1b9396383f9d8095528, https://www.openssl.org/news/secadv/20230719.txt	A-OPE-OPEN-020823/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. **CVE ID : CVE-2023-3446**		
Affected Version(s): 3.1.0					
N/A	19-Jul-2023	5.3	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fc9867c1e03c22ebf56943be205202e576aabf23, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8780a896543a654e757db1b9396383f9d8095528,	A-OPE-OPEN-020823/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be	https://www.openssl.org/news/secadv/20230719.txt	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. **CVE ID : CVE-2023-3446**		
Affected Version(s): 3.1.1					
N/A	19-Jul-2023	5.3	Issue summary: Checking excessively long DH keys or parameters may be very slow.	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=fc9867c1e03	A-OPE-OPEN-020823/384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the	c22ebf56943be205202e576aabf23, https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8780a896543a654e757db1b9396383f9d8095528, https://www.openssl.org/news/secadv/20230719.txt	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			not affected by this issue. **CVE ID : CVE-2023-3446**		
Vendor: Oracle					
Product: agile_plm					
Affected Version(s): 9.3.6					
N/A	18-Jul-2023	5.4	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: WebClient). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM accessible data as well as unauthorized read access to a subset of	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-AGIL-020823/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Agile PLM accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22039**		
Product: applications_framework					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.3.12					
N/A	18-Jul-2023	6.1	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.2.3-12.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products (scope change). Successful attacks of this	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-APPL-020823/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data as well as unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22042**		
Product: application_express					
Affected Version(s): From (including) 18.2 Up to (including) 22.1					
N/A	18-Jul-2023	9	Vulnerability in the Application Express Team Calendar Plugin product of Oracle Application Express (component: User Account). Supported versions that are affected are Application Express Team Calendar Plugin: 18.2-22.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Application Express	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-APPL-020823/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Team Calendar Plugin. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express Team Calendar Plugin, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Application Express Team Calendar Plugin. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21974**		
Affected Version(s): From (including) 18.2 Up to (including) 22.2					
N/A	18-Jul-2023	9	Vulnerability in the Application Express Customers Plugin product of Oracle Application Express (component: User Account). Supported versions that are affected are Application Express Customers Plugin: 18.2-22.2. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-APPL-020823/388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			low privileged attacker with network access via HTTP to compromise Application Express Customers Plugin. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express Customers Plugin, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Application Express Customers Plugin. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2023-21975**		
N/A	18-Jul-2023	5.6	Vulnerability in the Application Express Administration product of Oracle Application Express (component: None). Supported versions that are affected are Application Express Administration: 18.2-	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-APPL-020823/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Application Express Administration. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Application Express Administration accessible data as well as unauthorized read access to a subset of Application Express Administration accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Application Express Administration. CVSS 3.1 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2023-21983**		
Product: business_intelligence					
Affected Version(s): 6.4.0.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2023-22011**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22020**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Visual Analyzer). The supported version that is affected is 6.4.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22061**		
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22013**		
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22021**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/394
Affected Version(s): 7.0.0.0.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2023-22011**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	5.4	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22020**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22012**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/397
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22013**		
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 6.4.0.0.0 and 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22021**		
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). The supported version that is affected is 7.0.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-BUSI-020823/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22027**		
Product: database_server					
Affected Version(s): From (including) 19.3 Up to (including) 19.19					
N/A	18-Jul-2023	4.9	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Easily exploitable vulnerability allows high privileged attacker having SYSDBA privilege with network access via Oracle Net to compromise Unified Audit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Unified Audit accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts).	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-DATA-020823/401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-22034**		
N/A	18-Jul-2023	3.7	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Advanced Networking Option accessible data. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21949**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-DATA-020823/402
N/A	18-Jul-2023	3.1	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are	https://www.oracle.com/security-	A-ORA-DATA-020823/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected are 19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22052**	alerts/cpujul2023.html	
Affected Version(s): From (including) 21.3 Up to (including) 21.10					
N/A	18-Jul-2023	4.9	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Easily exploitable vulnerability allows high privileged attacker having SYSDBA privilege with network access via Oracle Net to	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-DATA-020823/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Unified Audit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Unified Audit accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-22034**		
N/A	18-Jul-2023	3.7	Vulnerability in the Advanced Networking Option component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Advanced Networking Option. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Advanced Networking Option accessible data. CVSS	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-DATA-020823/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-21949**		
N/A	18-Jul-2023	3.1	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.19 and 21.3-21.10. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22052**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-DATA-020823/406
Product: e-business_suite					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	6.1	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: iSurvey Module). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Scripting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Scripting accessible data as well as unauthorized read access to a subset of Oracle Scripting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-E-BU-020823/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22035**		
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Applications Technology product of Oracle E-Business Suite (component: Reports Configuration). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Technology accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-E-BU-020823/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22004		
Product: essbase					
Affected Version(s): 21.4.3.0.0					
N/A	18-Jul-2023	2.2	Vulnerability in Oracle Essbase (component: Security and Provisioning). The supported version that is affected is 21.4.3.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Essbase accessible data. CVSS 3.1 Base Score 2.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22010**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-ESSB-020823/409
Product: fusion_middleware					
Affected Version(s): * Up to (excluding) 11.1.2.3.1					
N/A	18-Jul-2023	6.5	Vulnerability in the Oracle Mobile Security Suite product of Oracle Fusion Middleware (component: Android Mobile Authenticator	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-FUSI-020823/410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			App). Supported versions that are affected are Prior to 11.1.2.3.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Mobile Security Suite executes to compromise Oracle Mobile Security Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Security Suite accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-21994**		
Product: graalvm					
Affected Version(s): 20.3.10					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Affected Version(s): 21.3.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: GraalVM Compiler). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22051**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data.	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Affected Version(s): 22.3.2					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1;	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data.	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: GraalVM Compiler). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22051**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Product: graalvm_for_jdk					
Affected Version(s): 17.0.7					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: GraalVM Compiler). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22051**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Affected Version(s): 20.0.1					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle	https://www.oracle.com	A-ORA-GRAA-020823/440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This	/security-alerts/cpujul2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: GraalVM Compiler). Supported versions that are affected are Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22051**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-GRAA-020823/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Product: health_sciences_applications					
Affected Version(s): 3.1.0.2					
N/A	18-Jul-2023	6.5	Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of Oracle Health Sciences	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-HEAL-020823/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22022**		
Affected Version(s): 3.1.1.3					
N/A	18-Jul-2023	6.5	Vulnerability in the Oracle Health Sciences Sciences Data Management Workbench product of	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-HEAL-020823/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22022**		
Affected Version(s): 3.2.0.0					
N/A	18-Jul-2023	6.5	Vulnerability in the Oracle Health Sciences Sciences Data Management	https://www.oracle.com/security-	A-ORA-HEAL-020823/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Workbench product of Oracle Health Sciences Applications (component: Blinding Functionality). Supported versions that are affected are 3.1.0.2, 3.1.1.3 and 3.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Health Sciences Sciences Data Management Workbench accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22022**	alerts/cpujul2023.html	
Product: hyperion					
Affected Version(s): 11.2.13.0.000					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	8.5	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Repository). The supported version that is affected is 11.2.13.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. While the vulnerability is in Oracle Hyperion Financial Reporting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-HYPE-020823/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:L/UI:N/S:C/C:H/I:N/A:L). **CVE ID : CVE-2023-22062**		
Product: hyperion_essbase_administration_services					
Affected Version(s): 21.4.3.0.0					
N/A	18-Jul-2023	6	Vulnerability in the Oracle Hyperion Essbase Administration Services product of Oracle Essbase (component: EAS Administration and EAS Console). The supported version that is affected is 21.4.3.0.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Essbase Administration Services executes to compromise Oracle Hyperion Essbase Administration Services. While the vulnerability is in Oracle Hyperion Essbase Administration Services, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-HYPE-020823/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to critical data or complete access to all Oracle Hyperion Essbase Administration Services accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2023-21961**		
Product: hyperion_workspace					
Affected Version(s): 11.2.13.0.000					
N/A	18-Jul-2023	7.6	Vulnerability in the Oracle Hyperion Workspace product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.2.13.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Workspace. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation,	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-HYPE-020823/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deletion or modification access to critical data or all Oracle Hyperion Workspace accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Workspace accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Workspace. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L). **CVE ID : CVE-2023-22060**		
Product: jdk					
Affected Version(s): 17.0.7					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle	https://www.oracle.com	A-ORA-JDK-020823/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also	/security-alerts/cpujul2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22045		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Affected Version(s): 20.0.1					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H /PR:N/UI:N/S:U/C:H/ I:N/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22041		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19,	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22006		
Affected Version(s): 1.8.0					
N/A	18-Jul-2023	5.9	Vulnerability in Oracle Java SE (component: JavaFX). The supported version that is affected is Oracle Java SE: 8u371. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-22043**		
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data.	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
Affected Version(s): 11.0.19					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1;	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JDK-020823/471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Product: jd_edwards_enterpriseone_orchestrator					
Affected Version(s): * Up to (excluding) 9.2.7.4					
N/A	18-Jul-2023	5.4	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product	https://www.oracle.com/security-	A-ORA-JD_E-020823/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Oracle JD Edwards (component: E1 IOT Orchestrator Security). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2023-22050**	alerts/cpujul2023.html	
Product: jd_edwards_enterpriseone_tools					
Affected Version(s): * Up to (excluding) 9.2.7.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	6.1	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are Prior to 9.2.7.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data as well as unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JD_E-020823/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2023-22055**		
Product: jre					
Affected Version(s): 17.0.7					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-	A-ORA-JRE-020823/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also	alerts/cpujul 2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22044		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Affected Version(s): 20.0.1					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-	A-ORA-JRE-020823/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically	alerts/cpujul 2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371,	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle	https://www.oracle.com/security-	A-ORA-JRE-020823/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients	alerts/cpujul 2023.html	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Affected Version(s): 1.8.0					
N/A	18-Jul-2023	5.9	Vulnerability in Oracle Java SE (component: JavaFX). The supported version that is affected is Oracle Java SE: 8u371. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2023-22043**		
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
Affected Version(s): 11.0.19					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1;	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-JRE-020823/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Product: mysql					
Affected Version(s): From (including) 5.0.0 Up to (including) 5.7.41					
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22007**		
Affected Version(s): From (including) 5.0.0 Up to (including) 5.7.42					
N/A	18-Jul-2023	5.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.42 and prior and 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector:	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H). **CVE ID : CVE-2023-22053**		
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.27					
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-21950**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/498
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.32					
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL	https://www.oracle.com/security-	A-ORA-MYSQ-020823/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(component: Server: Replication). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22007**	alerts/cpujul2023.html	
Affected Version(s): From (including) 8.0.0 Up to (including) 8.0.33					
N/A	18-Jul-2023	5.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.42 and prior and 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H). **CVE ID : CVE-2023-22053**		
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22008**		
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22046		
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22054**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/503
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.33 and prior. Easily exploitable	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22056**		
N/A	18-Jul-2023	4.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22057**		
N/A	18-Jul-2023	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22005		
N/A	18-Jul-2023	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22033**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/507
N/A	18-Jul-2023	4.4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows high privileged	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22058**		
N/A	18-Jul-2023	3.1	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 8.0.33 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22048**		
N/A	18-Jul-2023	2.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22038**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-MYSQ-020823/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: peoplesoft_enterprise					
Affected Version(s): 8.59					
N/A	18-Jul-2023	7.5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22047**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-PEOP-020823/511
Affected Version(s): 8.60					
N/A	18-Jul-2023	7.5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal).	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-PEOP-020823/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22047**		
Product: peoplesoft_enterprise_peopletools					
Affected Version(s): 8.59					
N/A	18-Jul-2023	8.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with logon to	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-PEOP-020823/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22014**		
Affected Version(s): 8.60					
N/A	18-Jul-2023	8.4	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.59 and 8.60. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-PEOP-020823/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22014**		
Product: self-service_human_resources					
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jul-2023	4.3	Vulnerability in the Oracle Self-Service Human Resources product of Oracle E-Business Suite (component: Workforce Management). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Self-Service Human Resources. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Self-Service Human Resources accessible data. CVSS	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-SELF-020823/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22009**		
Product: vm_virtualbox					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.1.46					
N/A	18-Jul-2023	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22018**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-VM_V-020823/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22017**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-VM_V-020823/517
N/A	18-Jul-2023	4.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core).	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-VM_V-020823/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22016**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.10					
N/A	18-Jul-2023	8.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-VM_V-020823/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Prior to 6.1.46 and Prior to 7.0.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22018**		
N/A	18-Jul-2023	5.5	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-VM_V-020823/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows VMs only. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22017**		
N/A	18-Jul-2023	4.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 6.1.46 and Prior to 7.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-VM_V-020823/521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22016**		
Product: weblogic_server					
Affected Version(s): 12.2.1.4.0					
N/A	18-Jul-2023	6.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-WEBL-020823/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2023-22040**		
N/A	18-Jul-2023	4.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.1.0.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 4.4 (Availability	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-WEBL-020823/523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22031**		
Affected Version(s): 14.1.1.0.0					
N/A	18-Jul-2023	6.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-WEBL-020823/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2023-22040**		
N/A	18-Jul-2023	4.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.1.0.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2023-22031**	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-WEBL-020823/525
Product: web_applications_desktop_integrator					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 12.2.3 Up to (including) 12.2.12					
N/A	18-Jul-2023	6.5	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: MS Excel Specific). Supported versions that are affected are 12.2.3-12.2.12. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Applications Desktop Integrator, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Web Applications Desktop Integrator accessible data as well as unauthorized read access to a subset of Oracle Web	https://www.oracle.com/security-alerts/cpujul2023.html	A-ORA-WEB_-020823/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Applications Desktop Integrator accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Web Applications Desktop Integrator. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2023-22037**		
Vendor: orjinyazilim					
Product: ats_pro					
Affected Version(s): * Up to (excluding) 20230714					
Authorization Bypass Through User-Controlled Key	17-Jul-2023	9.8	Authorization Bypass Through User-Controlled Key vulnerability in Origin Software ATS Pro allows Authentication Abuse, Authentication Bypass.This issue affects ATS Pro: before 20230714. **CVE ID : CVE-2023-2958**	N/A	A-ORJ-ATS_-020823/527
Vendor: paddlepaddle					
Product: paddlepaddle					
Affected Version(s): * Up to (excluding) 2.5.0					
Use After Free	26-Jul-2023	9.8	Use after free in paddle.diagonal in PaddlePaddle before 2.5.0. This resulted in	https://github.com/PaddlePaddle/Paddle/blob/de	A-PAD-PADD-020823/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a potentially exploitable condition. **CVE ID : CVE-2023-38669**	velop/security/advisory/pdsa-2023-001.md	
Out-of-bounds Write	26-Jul-2023	9.8	Heap buffer overflow in paddle.trace in PaddlePaddle before 2.5.0. This flaw can lead to a denial of service, information disclosure, or more damage is possible. **CVE ID : CVE-2023-38671**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-003.md	A-PAD-PADD-020823/529
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Jul-2023	9.8	PaddlePaddle before 2.5.0 has a command injection in fs.py. This resulted in the ability to execute arbitrary commands on the operating system. **CVE ID : CVE-2023-38673**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-005.md	A-PAD-PADD-020823/530
NULL Pointer Dereference	26-Jul-2023	7.5	Null pointer dereference in paddle.flip in PaddlePaddle before 2.5.0. This resulted in a runtime crash and denial of service. **CVE ID : CVE-2023-38670**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/pdsa-2023-002.md	A-PAD-PADD-020823/531
Divide By Zero	26-Jul-2023	7.5	FPE in paddle.trace in PaddlePaddle before 2.5.0. This flaw can cause a runtime crash and a denial of service. **CVE ID : CVE-2023-38672**	https://github.com/PaddlePaddle/Paddle/blob/develop/security/advisory/	A-PAD-PADD-020823/532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				pdsa-2023-004.md	
Vendor: Panasonic					
Product: control_fpwin_pro					
Affected Version(s): * Up to (including) 7.6.0.3					
Out-of-bounds Write	21-Jul-2023	7.8	A stack-based buffer overflow in Panasonic Control FPWIN Pro versions 7.6.0.3 and all previous versions may allow arbitrary code execution when opening specially crafted project files. **CVE ID : CVE-2023-28728**	N/A	A-PAN-CONT-020823/533
Access of Resource Using Incompatible Type ('Type Confusion')	21-Jul-2023	7.8	A type confusion vulnerability in Panasonic Control FPWIN Pro versions 7.6.0.3 and all previous versions may allow arbitrary code execution when opening specially crafted project files. **CVE ID : CVE-2023-28729**	N/A	A-PAN-CONT-020823/534
Out-of-bounds Write	21-Jul-2023	7.8	A memory corruption vulnerability Panasonic Control FPWIN Pro versions 7.6.0.3 and all previous versions may allow arbitrary code execution when opening specially crafted project files.	N/A	A-PAN-CONT-020823/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28730		
Vendor: Papercut					
Product: papercut_mf					
Affected Version(s): * Up to (excluding) 22.1.3					
Unrestricted Upload of File with Dangerous Type	25-Jul-2023	7.5	An authentication bypass exists in PaperCut NG versions 22.0.12 and prior that could allow a remote, unauthenticated attacker to upload arbitrary files to the PaperCut NG host's file storage. This could exhaust system resources and prevent the service from operating as expected. **CVE ID : CVE-2023-3486**	https://www.papercut.com/kb/Main/SecurityBulletinJuly2023/	A-PAP-PAPE-020823/536
Product: papercut_ng					
Affected Version(s): * Up to (excluding) 22.1.3					
Unrestricted Upload of File with Dangerous Type	25-Jul-2023	7.5	An authentication bypass exists in PaperCut NG versions 22.0.12 and prior that could allow a remote, unauthenticated attacker to upload arbitrary files to the PaperCut NG host's file storage. This could exhaust system resources and prevent the service from operating as expected.	https://www.papercut.com/kb/Main/SecurityBulletinJuly2023/	A-PAP-PAPE-020823/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3486		
Vendor: paulprinting_project					
Product: paulprinting					
Affected Version(s): 2018					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in PaulPrinting CMS 2018. Affected is an unknown function of the file /account/delivery of the component Search. The manipulation of the argument s 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-235056. **CVE ID : CVE-2023-3789**	N/A	A-PAU-PAUL-020823/538
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	5.4	A vulnerability was found in PaulPrinting CMS 2018. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument firstname/lastname/address/city/state leads to cross site scripting. The attack may be launched	N/A	A-PAU-PAUL-020823/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235052. **CVE ID : CVE-2023-3785**		
Vendor: phpscriptpoint					
Product: bloodbank					
Affected Version(s): 1.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jul-2023	9.8	A vulnerability classified as critical has been found in phpscriptpoint BloodBank 1.1. Affected is an unknown function of the file /search of the component POST Parameter Handler. The manipulation of the argument country/city/blood_group_id leads to sql injection. It is possible to launch the attack remotely. VDB-235206 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3854**	N/A	A-PHP-BLOO-020823/540
Improper Neutralization of Input	23-Jul-2023	6.1	A vulnerability was found in phpscriptpoint BloodBank 1.1. It has	N/A	A-PHP-BLOO-020823/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			been rated as problematic. This issue affects some unknown processing of the file page.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-235205 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3853**		
Product: car_listing					
Affected Version(s): 1.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jul-2023	9.8	A vulnerability was found in phpscriptpoint Car Listing 1.6 and classified as critical. This issue affects some unknown processing of the file /search.php of the component GET Parameter Handler. The manipulation of the argument brand_id/model_id/car_condition/car_category_id/body_type_id/fuel_type_id/transmission_type_id/year/mileage_start/mileage_end/country/state/city leads to sql injection.	N/A	A-PHP-CAR_-020823/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-235211. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3859**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	6.1	A vulnerability has been found in phpscriptpoint Car Listing 1.6 and classified as problematic. This vulnerability affects unknown code of the file /search.php. The manipulation of the argument country/state/city leads to cross site scripting. The attack can be initiated remotely. VDB-235210 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3858**	N/A	A-PHP-CAR_-020823/543
Product: ecommerce					
Affected Version(s): 1.15					
Improper Neutralizat	24-Jul-2023	6.1	A vulnerability, which was classified as	N/A	A-PHP-ECOM-020823/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			problematic, has been found in phpscriptpoint Ecommerce 1.15. Affected by this issue is some unknown functionality of the file /blog-single.php. The manipulation of the argument slug leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235208. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3856**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	6.1	A vulnerability, which was classified as problematic, was found in phpscriptpoint Ecommerce 1.15. This affects an unknown part of the file /product.php. The manipulation of the argument id leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-235209 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure	N/A	A-PHP-ECOM-020823/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			but did not respond in any way. **CVE ID : CVE-2023-3857**		
Product: insurance					
Affected Version(s): 1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	6.1	A vulnerability was found in phpscriptpoint Insurance 1.2. It has been classified as problematic. Affected is an unknown function of the file /page.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-235212. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3860**	N/A	A-PHP-INSU-020823/546
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	6.1	A vulnerability was found in phpscriptpoint Insurance 1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /search.php. The manipulation leads to cross site scripting. The attack can be launched remotely.	N/A	A-PHP-INSU-020823/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The identifier VDB-235213 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3861**		
Product: jobseeker					
Affected Version(s): 1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	6.1	A vulnerability classified as problematic was found in phpscriptpoint JobSeeker 1.5. Affected by this vulnerability is an unknown functionality of the file /search-result.php. The manipulation of the argument kw/lc/ct/cp/p leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-235207. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3855**	N/A	A-PHP-JOBS-020823/548
Product: lawyer					
Affected Version(s): 1.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	A vulnerability was found in phpscriptpoint Lawyer 1.6 and classified as problematic. Affected by this issue is some unknown functionality of the file page.php. The manipulation leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-235400. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3944**	N/A	A-PHP-LAWY-020823/549
Vendor: Pimcore					
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.6.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jul-2023	7.2	SQL Injection in GitHub repository pimcore/pimcore prior to 10.6.4. **CVE ID : CVE-2023-3820**	https://github.com/pimcore/pimcore/commit/e641968979d4a2377bbea5e2a76bdede040d0b97, https://huntr.dev/bounties/b00a38b6-d040-494d-bf46-38f46ac1a1db	A-PIM-PIMC-020823/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	21-Jul-2023	6.5	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository pimcore/pimcore prior to 10.6.4. **CVE ID : CVE-2023-3819**	https://github.com/pimcore/pimcore/commit/0237527b3244d251fa5ecd4912dfe4f8b2125c54, https://huntr.dev/bounties/be5e4d4c-1b0b-4c01-a1fc-00533135817c	A-PIM-PIMC-020823/551
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository pimcore/pimcore prior to 10.6.4. **CVE ID : CVE-2023-3822**	https://github.com/pimcore/pimcore/commit/d75888a9b14baaad591548463cca09dfd1395236, https://huntr.dev/bounties/2a3a13fe-2a9a-4d1a-8814-fd8ed1e3b1d5	A-PIM-PIMC-020823/552
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.6.4. **CVE ID : CVE-2023-3821**	https://huntr.dev/bounties/599ba4f6-c900-4161-9127-f1e6a6e29aaa, https://github.com/pimcore/pimcore/commit/92811f07d39e4ad95c9200	A-PIM-PIMC-020823/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				3868f5f7309489d79c	
Vendor: Pixman					
Product: pixman					
Affected Version(s): -					
Divide By Zero	17-Jul-2023	6.5	stress-test master commit e4c878 was discovered to contain a FPE vulnerability via the component combine_inner at /pixman-combine-float.c. **CVE ID : CVE-2023-37769**	N/A	A-PIX-PIXM-020823/554
Vendor: pluginforage					
Product: woocommerce_product_categories_selection_widget					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in PluginForage WooCommerce Product Categories Selection Widget plugin <= 2.0 versions. **CVE ID : CVE-2023-33925**	N/A	A-PLU-WOOC-020823/555
Vendor: pluginpress					
Product: shortcode_imdb					
Affected Version(s): * Up to (including) 6.0.8					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kemal YAZICI - PluginPress Shortcode IMDB plugin <= 6.0.8 versions.	N/A	A-PLU-SHOR-020823/556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37892		
Vendor: pointware					
Product: easyinventory					
Affected Version(s): 1.0.12.0					
Unquoted Search Path or Element	23-Jul-2023	7.8	A vulnerability was found in Pointware EasyInventory 1.0.12.0 and classified as critical. This issue affects some unknown processing of the file C:\Program Files (x86)\EasyInventory\Easy2W.exe. The manipulation leads to unquoted search path. Attacking locally is a requirement. The identifier VDB-235193 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3842**	N/A	A-POI-EASY-020823/557
Vendor: premio					
Product: chaty					
Affected Version(s): * Up to (excluding) 3.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	4.8	The Floating Chat Widget WordPress plugin before 3.1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-	N/A	A-PRE-CHAT-020823/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-3245**		
Product: my_sticky_elements					
Affected Version(s): * Up to (excluding) 2.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	4.8	The All-in-one Floating Contact Form WordPress plugin before 2.1.2 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 even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-3248**	N/A	A-PRE-MY_S-020823/559
Vendor: premmerce					
Product: premmerce					
Affected Version(s): * Up to (including) 1.3.17					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Premmerce plugin <= 1.3.17 versions. **CVE ID : CVE-2023-23719**	N/A	A-PRE-PREM-020823/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Prestashop					
Product: amazon					
Affected Version(s): * Up to (excluding) 5.2.24					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jul-2023	5.3	An issue in /functions/fbaorder.php of Prestashop amazon before v5.2.24 allows attackers to execute a directory traversal attack. **CVE ID : CVE-2023-33777**	https://addons.prestashop.com/fr/marketplace/2501-amazon-market-place.html	A-PRE-AMAZ-020823/561
Product: payplug					
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.8.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jul-2023	9.8	An SQL injection vulnerability in the Payplug (payplug) module for PrestaShop, in versions 3.6.0, 3.6.1, 3.6.2, 3.6.3, 3.7.0 and 3.7.1, allows remote attackers to execute arbitrary SQL commands via the ajax.php front controller. **CVE ID : CVE-2023-30153**	https://security.friendsofpresta.org/module/2023/07/18/payplug.html	A-PRE-PAYP-020823/562
Vendor: Progress					
Product: chef_infra_server					
Affected Version(s): From (including) 12.0.0 Up to (excluding) 15.7.0					
Insecure Storage of Sensitive Information	17-Jul-2023	5.5	Progress Chef Infra Server before 15.7 allows a local attacker to exploit a /var/opt/opscode/local-mode-cache/backup world-readable temporary	N/A	A-PRO-CHEF-020823/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			backup path to access sensitive information, resulting in the disclosure of all indexed node data, because OpenSearch credentials are exposed. (The data typically includes credentials for additional systems.) The attacker must wait for an admin to run the "chef-server-ctl reconfigure" command. **CVE ID : CVE-2023-28864**		
Vendor: querlo					
Product: chatbot					
Affected Version(s): * Up to (including) 1.2.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	5.4	The Querlo Chatbot WordPress plugin through 1.2.4 does not escape or sanitize chat messages, leading to a stored Cross-Site Scripting vulnerability. **CVE ID : CVE-2023-3418**	N/A	A-QUE-CHAT-020823/564
Vendor: radiustheme					
Product: classified_listing_pro_-_classified_ads_\&_business_directory					
Affected Version(s): * Up to (including) 2.4.5					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in RadiusTheme Classified Listing	N/A	A-RAD-CLAS-020823/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 2.4.5 versions. **CVE ID : CVE-2023-37387**		
Vendor: really-simple-plugins					
Product: recipe_maker_for_your_food_blog_from_zip_recipes					
Affected Version(s): * Up to (excluding) 8.0.8					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Really Simple Plugins Recipe Maker For Your Food Blog from Zip Recipes plugin <= 8.0.7 versions. **CVE ID : CVE-2023-35089**	N/A	A-REA-RECI-020823/566
Vendor: recent_posts_slider_project					
Product: recent_posts_slider					
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Neha Goel Recent Posts Slider plugin <= 1.1 versions. **CVE ID : CVE-2023-35043**	N/A	A-REC-RECE-020823/567
Vendor: Redhat					
Product: openshift					
Affected Version(s): -					
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368, https://ww	A-RED-OPEN-020823/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	w.ibm.com/support/pages/node/7010895	
Improper Authentication	17-Jul-2023	5.3	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380. **CVE ID : CVE-2023-35901**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259380, https://www.ibm.com/support/pages/node/7012317	A-RED-OPEN-020823/569
Product: openstack_platform					
Affected Version(s): 13.0					
Uncontrolled Resource Consumption	25-Jul-2023	6.5	An uncontrolled resource consumption flaw was found in openstack-neutron. This flaw allows a remote authenticated user to query a list of security groups for an invalid project. This issue creates resources that are unconstrained by the user's quota. If a malicious user were to submit a significant number of requests, this could lead to a denial of service.	https://bugzilla.redhat.com/show_bug.cgi?id=2222270, https://access.redhat.com/security/cve/CVE-2023-3637, https://access.redhat.com/errata/RHSA-2023:4283	A-RED-OPEN-020823/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3637		
Affected Version(s): 16.2					
Uncontrolled Resource Consumption	25-Jul-2023	6.5	An uncontrolled resource consumption flaw was found in openstack-neutron. This flaw allows a remote authenticated user to query a list of security groups for an invalid project. This issue creates resources that are unconstrained by the user's quota. If a malicious user were to submit a significant number of requests, this could lead to a denial of service. **CVE ID : CVE-2023-3637**	https://bugzilla.redhat.com/show_bug.cgi?id=2222270, https://access.redhat.com/security/cve/CVE-2023-3637, https://access.redhat.com/errata/RHSA-2023:4283	A-RED-OPEN-020823/571
Product: storage					
Affected Version(s): 3.0					
N/A	20-Jul-2023	5.9	A vulnerability was found in Samba's SMB2 packet signing mechanism. The SMB2 packet signing is not enforced if an admin configured "server signing = required" or for SMB2 connections to Domain Controllers where SMB2 packet signing is mandatory. This flaw allows an attacker to perform attacks, such as a man-in-the-middle attack, by intercepting the	https://www.samba.org/samba/security/CVE-2023-3347.html	A-RED-STOR-020823/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network traffic and modifying the SMB2 messages between client and server, affecting the integrity of the data. **CVE ID : CVE-2023-3347**		
N/A	20-Jul-2023	5.3	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path. **CVE ID : CVE-2023-34968**	https://www.samba.org/samba/security/CVE-2023-34968.html	A-RED-STOR-020823/573
Vendor: replace_word_project					
Product: replace_word					
Affected Version(s): * Up to (including) 2.1					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in David Pokorny Replace Word plugin <= 2.1 versions. **CVE ID : CVE-2023-37973**	N/A	A-REP-REPL-020823/574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Rockwellautomation					
Product: thinmanager					
Affected Version(s): From (including) 13.0.0 Up to (including) 13.0.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Jul-2023	6.5	An executable used in Rockwell Automation ThinManager ThinServer can be configured to enable an API feature in the HTTPS Server Settings. This feature is disabled by default. When the API is enabled and handling requests, a path traversal vulnerability exists that allows a remote actor to leverage the privileges of the server's file system and read arbitrary files stored in it. A malicious user could exploit this vulnerability by executing a path that contains manipulating variables. **CVE ID : CVE-2023-2913**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140160	A-ROC-THIN-020823/575
Vendor: royal-elementor-addons					
Product: royal_elementor_addons					
Affected Version(s): * Up to (including) 1.3.70					
Exposure of Sensitive Information to an Unauthorized Actor	18-Jul-2023	5.3	The Royal Elementor Addons plugin for WordPress is vulnerable to unauthenticated API key disclosure in versions up to, and	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=	A-ROY-ROYA-020823/576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 1.3.70 due to the plugin adding the API key to the source code of any page running the MailChimp block. This makes it possible for unauthenticated attackers to obtain a site's MailChimp API key. We recommend resetting any MailChimp API keys if running a vulnerable version of this plugin with the MailChimp block enabled as the API key may have been compromised. **CVE ID : CVE-2023-3709**	2938619%40royal-elementor-addons&new=2936984%40royal-elementor-addons&sfp_email=&sfph_mail=	
Vendor: ruoyi					
Product: ruoyi					
Affected Version(s): * Up to (including) 4.7.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2023	6.1	A vulnerability, which was classified as problematic, has been found in y_project RuoYi up to 4.7.7. Affected by this issue is the function uploadFilesPath of the component File Upload. The manipulation of the argument originalFilenames leads to cross site scripting. The attack may be launched remotely. VDB-235118 is the	N/A	A-RUO-RUOY-020823/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier assigned to this vulnerability. **CVE ID : CVE-2023-3815**		
Vendor: Samba					
Product: samba					
Affected Version(s): * Up to (excluding) 4.16.11					
Loop with Unreachable Exit Condition ('Infinite Loop')	20-Jul-2023	7.5	An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial of service condition. **CVE ID : CVE-2023-34966**	https://www.samba.org/samba/security/CVE-2023-34966	A-SAM-SAMB-020823/578
Access of Resource Using Incompatible Type	20-Jul-2023	5.3	A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When	https://www.samba.org/samba/security/CVE-	A-SAM-SAMB-020823/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the mdssvc protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc worker process, affecting all other clients this worker serves. **CVE ID : CVE-2023-34967**	2023-34967.html	
N/A	20-Jul-2023	5.3	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba	https://www.samba.org/samba/security/CVE-	A-SAM-SAMB-020823/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path. **CVE ID : CVE-2023-34968**	2023-34968.html	
Affected Version(s): From (including) 4.17.0 Up to (excluding) 4.17.10					
Loop with Unreachable Exit Condition ('Infinite Loop')	20-Jul-2023	7.5	An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting	https://www.samba.org/samba/security/CVE-2023-34966	A-SAM-SAMB-020823/581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in a denial of service condition. **CVE ID : CVE-2023-34966**		
N/A	20-Jul-2023	5.9	A vulnerability was found in Samba's SMB2 packet signing mechanism. The SMB2 packet signing is not enforced if an admin configured "server signing = required" or for SMB2 connections to Domain Controllers where SMB2 packet signing is mandatory. This flaw allows an attacker to perform attacks, such as a man-in-the-middle attack, by intercepting the network traffic and modifying the SMB2 messages between client and server, affecting the integrity of the data. **CVE ID : CVE-2023-3347**	https://www.samba.org/samba/security/CVE-2023-3347.html	A-SAM-SAMB-020823/582
Access of Resource Using Incompatible Type ('Type Confusion')	20-Jul-2023	5.3	A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types	https://www.samba.org/samba/security/CVE-2023-34967.html	A-SAM-SAMB-020823/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the mdssvc protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc worker process, affecting all other clients this worker serves. **CVE ID : CVE-2023-34967**		
N/A	20-Jul-2023	5.3	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC	https://www.samba.org/samba/security/CVE-2023-34968.html	A-SAM-SAMB-020823/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to view the information that is part of the disclosed path. **CVE ID : CVE-2023-34968**		
Affected Version(s): From (including) 4.18.0 Up to (excluding) 4.18.5					
Loop with Unreachable Exit Condition ('Infinite Loop')	20-Jul-2023	7.5	An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial of service condition. **CVE ID : CVE-2023-34966**	https://www.samba.org/samba/security/CVE-2023-34966	A-SAM-SAMB-020823/585
N/A	20-Jul-2023	5.9	A vulnerability was found in Samba's SMB2 packet signing mechanism. The SMB2 packet signing is not	https://www.samba.org/samba/security/CVE-	A-SAM-SAMB-020823/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enforced if an admin configured "server signing = required" or for SMB2 connections to Domain Controllers where SMB2 packet signing is mandatory. This flaw allows an attacker to perform attacks, such as a man-in-the-middle attack, by intercepting the network traffic and modifying the SMB2 messages between client and server, affecting the integrity of the data. **CVE ID : CVE-2023-3347**	2023-3347.html	
Access of Resource Using Incompatible Type ('Type Confusion')	20-Jul-2023	5.3	A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the mdssvc protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a	https://www.samba.org/samba/security/CVE-2023-34967.html	A-SAM-SAMB-020823/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc worker process, affecting all other clients this worker serves. **CVE ID : CVE-2023-34967**		
N/A	20-Jul-2023	5.3	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path. **CVE ID : CVE-2023-34968**	https://www.samba.org/samba/security/CVE-2023-34968.html	A-SAM-SAMB-020823/588
Vendor: secomea					
Product: sitemanager_embedded					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 11.0					
Use After Free	17-Jul-2023	7.5	Use After Free vulnerability in Secomea SiteManager Embedded allows Obstruction. **CVE ID : CVE-2023-2912**	https://www.secomea.com/support/cybersecurity-advisory/	A-SEC-SITE-020823/589
Vendor: smart_youtube_pro_project					
Product: smart_youtube_pro					
Affected Version(s): * Up to (including) 4.3					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Vladimir Prelovac Smart YouTube PRO plugin <= 4.3 versions. **CVE ID : CVE-2023-25475**	N/A	A-SMA-SMAR-020823/590
Vendor: social_media_icons_widget_project					
Product: social_media_icons_widget					
Affected Version(s): * Up to (including) 1.6					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in akhlesh-nagar, a.Ankit Social Media Icons Widget plugin <= 1.6 versions. **CVE ID : CVE-2023-25036**	N/A	A-SOC-SOCI-020823/591
Vendor: Solarwinds					
Product: database_performance_analyzer					
Affected Version(s): * Up to (excluding) 2023.2.100					
Improper Neutralization of Input	18-Jul-2023	6.1	XSS attack was possible in DPA 2023.2 due to	https://www.solarwinds.com/trust-center/secur	A-SOL-DATA-020823/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			insufficient input validation **CVE ID : CVE-2023-33231**	ity-advisories/CVE-2023-33231	
Vendor: solwininfotech					
Product: user_activity_log					
Affected Version(s): * Up to (excluding) 1.6.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Jul-2023	7.2	The User Activity Log WordPress plugin before 1.6.3 does not properly sanitise and escape the `txtsearch` parameter before using it in a SQL statement in some admin pages, leading to a SQL injection exploitable by high privilege users such as admin. **CVE ID : CVE-2023-2761**	N/A	A-SOL-USER-020823/593
Vendor: sourcecodester_house_rental_and_property_listing_project					
Product: house_rental_and_property_listing					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2023	9.8	A vulnerability, which was classified as critical, has been found in SourceCodester House Rental and Property Listing 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument keywords/location leads to sql injection. The attack may be	N/A	A-SOU-HOUS-020823/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-234245 was assigned to this vulnerability. **CVE ID : CVE-2023-3694**		
Vendor: squareup					
Product: okhttp					
Affected Version(s): *					
N/A	19-Jul-2023	5.9	DoS of the OkHttp client when using a BrotliInterceptor and surfing to a malicious web server, or when an attacker can perform MitM to inject a Brotli zip-bomb into an HTTP response **CVE ID : CVE-2023-3782**	https://github.com/square/okhttp/issues/7738	A-SQU-OKHT-020823/595
Vendor: steelseries					
Product: gg					
Affected Version(s): 36.0.0					
N/A	20-Jul-2023	8.8	An issue was discovered in SteelSeries GG 36.0.0. An attacker can change values in an unencrypted database that is writable for all users on the computer, in order to trigger code execution with higher privileges.	N/A	A-STE-GG-020823/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31462		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jul-2023	7.5	Attackers can exploit an open API listener on SteelSeries GG 36.0.0 to create a sub-application that will be executed automatically from a controlled location, because of a path traversal vulnerability. **CVE ID : CVE-2023-31461**	N/A	A-STE-GG-020823/597
Vendor: superstorefinder					
Product: super_store_finder					
Affected Version(s): 3.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2023	9.8	A vulnerability was found in Super Store Finder 3.6. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php of the component POST Parameter Handler. The manipulation of the argument products leads to sql injection. The attack can be launched remotely. The identifier VDB-234421 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-SUP-SUPE-020823/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3751		
Vendor: supsystic					
Product: popup					
Affected Version(s): * Up to (excluding) 1.10.19					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	17-Jul-2023	9.8	The Popup by Supsystic WordPress plugin before 1.10.19 has a prototype pollution vulnerability that could allow an attacker to inject arbitrary properties into Object.prototype. **CVE ID : CVE-2023-3186**	N/A	A-SUP-POPU-020823/599
Vendor: tduckcloud					
Product: tduck-platform					
Affected Version(s): 4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Jul-2023	6.1	An arbitrary file upload vulnerability in tduck-platform v4.0 allows attackers to execute arbitrary code via a crafted HTML file. **CVE ID : CVE-2023-37733**	N/A	A-TDU-TDUC-020823/600
Vendor: Tibco					
Product: ebx_add-ons					
Affected Version(s): * Up to (including) 4.5.17					
Improper Neutralization of Special Elements used in an SQL Command	19-Jul-2023	8.8	The Data Exchange Add-on component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an easily exploitable vulnerability that allows a low	https://www.tibco.com/services/support/advisories	A-TIB-EBX_-020823/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			privileged user with import permissions and network access to the EBX server to execute arbitrary SQL statements on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 4.5.17 and below, versions 5.6.2 and below, version 6.1.0. **CVE ID : CVE-2023-26217**		
Affected Version(s): 6.1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2023	8.8	The Data Exchange Add-on component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an easily exploitable vulnerability that allows a low privileged user with import permissions and network access to the EBX server to execute arbitrary SQL statements on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 4.5.17 and below, versions 5.6.2 and below, version 6.1.0. **CVE ID : CVE-2023-26217**	https://www.tibco.com/services/support/advisories	A-TIB-EBX_-020823/602
Affected Version(s): From (including) 5.0.0 Up to (including) 5.6.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2023	8.8	The Data Exchange Add-on component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains an easily exploitable vulnerability that allows a low privileged user with import permissions and network access to the EBX server to execute arbitrary SQL statements on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions 4.5.17 and below, versions 5.6.2 and below, version 6.1.0. **CVE ID : CVE-2023-26217**	https://www.tibco.com/services/support/advisories	A-TIB-EBX_-020823/603
Vendor: tiva_events_calendar_project					
Product: tiva_events_calendar					
Affected Version(s): 1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	5.4	A vulnerability classified as problematic was found in Codecanyon Tiva Events Calender 1.4. This vulnerability affects unknown code. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be	N/A	A-TIV-TIVA-020823/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. VDB-235054 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3787**		
Vendor: travelable_trek_management_solution_project					
Product: travelable_trek_management_solution					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-2023	4.7	A vulnerability was found in Travelmate Travelable Trek Management Solution 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Comment Box Handler. The manipulation of the argument comment leads to cross site scripting. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. VDB-235214 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3862**	N/A	A-TRA-TRAV-020823/605
Vendor: ultimatemember					
Product: ultimate_member					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.6.0					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ultimate Member plugin <= 2.6.0 versions. **CVE ID : CVE-2023-31216**	N/A	A-ULT-ULTI-020823/606
Vendor: uxblondon					
Product: boom_cms					
Affected Version(s): 8.0.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	5.4	A vulnerability has been found in Boom CMS 8.0.7 and classified as problematic. Affected by this vulnerability is the function add of the component assets-manager. The manipulation of the argument title/description 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-235057 was assigned to this vulnerability. **CVE ID : CVE-2023-3790**	N/A	A-UXB-BOOM-020823/607
Vendor: vanderbilt					
Product: redcap					
Affected Version(s): * Up to (excluding) 12.0.26					
Improper Neutralizat	25-Jul-2023	2.7	REDCap 12.0.26 LTS and 12.3.2 Standard	N/A	A-VAN-REDC-020823/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			allows SQL Injection via scheduling, repeatforms, purpose, app_title, or randomization. **CVE ID : CVE-2023-37361**		
Affected Version(s): * Up to (excluding) 12.3.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Jul-2023	2.7	REDCap 12.0.26 LTS and 12.3.2 Standard allows SQL Injection via scheduling, repeatforms, purpose, app_title, or randomization. **CVE ID : CVE-2023-37361**	N/A	A-VAN-REDC-020823/609
Vendor: Veritas					
Product: infoscale_operations_manager					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 8.0.0.410					
Unrestricted Upload of File with Dangerous Type	17-Jul-2023	8.8	The XPRTLD web application in Veritas InfoScale Operations Manager (VIOM) before 8.0.0.410 allows an authenticated attacker to upload all types of files to the server. An authenticated attacker can then execute the malicious file to perform command execution on the remote server. **CVE ID : CVE-2023-38404**	https://www.veritas.com/content/support/en_US/security/VTS23-009	A-VER-INFO-020823/610
Vendor: vibethemes					
Product: vslider					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 4.1.2					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Mr.Vibe vSlider Multi Image Slider for WordPress plugin <= 4.1.2 versions. **CVE ID : CVE-2023-22672**	N/A	A-VIB-VSLI-020823/611
Vendor: vm2_project					
Product: vm2					
Affected Version(s): * Up to (including) 3.9.19					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Jul-2023	9.8	vm2 is an open source vm/sandbox for Node.js. In vm2 for versions up to and including 3.9.19, Node.js custom inspect function allows attackers to escape the sandbox and run arbitrary code. This may result in Remote Code Execution, assuming the attacker has arbitrary code execution primitive inside the context of vm2 sandbox. There are no patches and no known workarounds. Users are advised to find an alternative software. **CVE ID : CVE-2023-37903**	https://github.com/patriksimek/vm2/security/advisories/GHSA-g644-9gfx-q4q4	A-VM2-VM2-020823/612
Vendor: Vmware					
Product: spring_hateoas					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.5.5					
Improper Encoding or Escaping of Output	17-Jul-2023	5.3	Reactive web applications that use Spring HATEOAS to produce hypermedia-based responses might be exposed to malicious forwarded headers if they are not behind a trusted proxy that ensures correctness of such headers, or if they don't have anything else in place to handle (and possibly discard) forwarded headers either in WebFlux or at the level of the underlying HTTP server. For the application to be affected, it needs to satisfy the following requirements: * It needs to use the reactive web stack (Spring WebFlux) and Spring HATEOAS to create links in hypermedia-based responses. * The application infrastructure does not guard against clients submitting (X-)Forwarded... headers. **CVE ID : CVE-2023-34036**	https://spring.io/security/cve-2023-34036	A-VMW-SPRI-020823/613
Affected Version(s): 2.1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	17-Jul-2023	5.3	Reactive web applications that use Spring HATEOAS to produce hypermedia-based responses might be exposed to malicious forwarded headers if they are not behind a trusted proxy that ensures correctness of such headers, or if they don't have anything else in place to handle (and possibly discard) forwarded headers either in WebFlux or at the level of the underlying HTTP server. For the application to be affected, it needs to satisfy the following requirements: * It needs to use the reactive web stack (Spring WebFlux) and Spring HATEOAS to create links in hypermedia-based responses. * The application infrastructure does not guard against clients submitting (X-)Forwarded... headers. **CVE ID : CVE-2023-34036**	https://spring.io/security/cve-2023-34036	A-VMW-SPRI-020823/614
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.0.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Encoding or Escaping of Output	17-Jul-2023	5.3	Reactive web applications that use Spring HATEOAS to produce hypermedia-based responses might be exposed to malicious forwarded headers if they are not behind a trusted proxy that ensures correctness of such headers, or if they don't have anything else in place to handle (and possibly discard) forwarded headers either in WebFlux or at the level of the underlying HTTP server. For the application to be affected, it needs to satisfy the following requirements: * It needs to use the reactive web stack (Spring WebFlux) and Spring HATEOAS to create links in hypermedia-based responses. * The application infrastructure does not guard against clients submitting (X-)Forwarded... headers. **CVE ID : CVE-2023-34036**	https://spring.io/security/cve-2023-34036	A-VMW-SPRI-020823/615
Product: spring_security					
Affected Version(s): From (including) 5.6.0 Up to (excluding) 5.6.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jul-2023	9.8	Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass. **CVE ID : CVE-2023-34034**	https://spring.io/security/cve-2023-34034	A-VMW-SPRI-020823/616
Affected Version(s): From (including) 5.7.0 Up to (excluding) 5.7.10					
N/A	19-Jul-2023	9.8	Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass. **CVE ID : CVE-2023-34034**	https://spring.io/security/cve-2023-34034	A-VMW-SPRI-020823/617
Affected Version(s): From (including) 5.8.0 Up to (excluding) 5.8.5					
N/A	19-Jul-2023	9.8	Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass.	https://spring.io/security/cve-2023-34034	A-VMW-SPRI-020823/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34034		
Incorrect Authorization	18-Jul-2023	5.3	Spring Security versions 5.8 prior to 5.8.5, 6.0 prior to 6.0.5, and 6.1 prior to 6.1.2 could be susceptible to authorization rule misconfiguration if the application uses requestMatchers(String) and multiple servlets, one of them being Spring MVC's DispatcherServlet. (DispatcherServlet is a Spring MVC component that maps HTTP endpoints to methods on @Controller-annotated classes.) Specifically, an application is vulnerable when all of the following are true: * Spring MVC is on the classpath * Spring Security is securing more than one servlet in a single application (one of them being Spring MVC's DispatcherServlet) * The application uses requestMatchers(String) to refer to endpoints that are not Spring MVC endpoints	https://spring.io/security/cve-2023-34035	A-VMW-SPRI-020823/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An application is not vulnerable if any of the following is true: * The application does not have Spring MVC on the classpath * The application secures no servlets other than Spring MVC's DispatcherServlet * The application uses requestMatchers(String) only for Spring MVC endpoints **CVE ID : CVE-2023-34035**		
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.0.5					
N/A	19-Jul-2023	9.8	Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass. **CVE ID : CVE-2023-34034**	https://spring.io/security/cve-2023-34034	A-VMW-SPRI-020823/620
Incorrect Authorization	18-Jul-2023	5.3	Spring Security versions 5.8 prior to 5.8.5, 6.0 prior to 6.0.5, and 6.1 prior to 6.1.2 could be susceptible to authorization rule misconfiguration if the application uses	https://spring.io/security/cve-2023-34035	A-VMW-SPRI-020823/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requestMatchers(String) and multiple servlets, one of them being Spring MVC's DispatcherServlet. (DispatcherServlet is a Spring MVC component that maps HTTP endpoints to methods on @Controller-annotated classes.) Specifically, an application is vulnerable when all of the following are true: * Spring MVC is on the classpath * Spring Security is securing more than one servlet in a single application (one of them being Spring MVC's DispatcherServlet) * The application uses requestMatchers(String) to refer to endpoints that are not Spring MVC endpoints An application is not vulnerable if any of the following is true: * The application does not have Spring MVC on the classpath * The application secures no servlets other than Spring		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MVC's DispatcherServlet * The application uses requestMatchers(String) only for Spring MVC endpoints **CVE ID : CVE-2023-34035**		
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.2					
N/A	19-Jul-2023	9.8	Using "**" as a pattern in Spring Security configuration for WebFlux creates a mismatch in pattern matching between Spring Security and Spring WebFlux, and the potential for a security bypass. **CVE ID : CVE-2023-34034**	https://spring.io/security/cve-2023-34034	A-VMW-SPRI-020823/622
Incorrect Authorization	18-Jul-2023	5.3	Spring Security versions 5.8 prior to 5.8.5, 6.0 prior to 6.0.5, and 6.1 prior to 6.1.2 could be susceptible to authorization rule misconfiguration if the application uses requestMatchers(String) and multiple servlets, one of them being Spring MVC's DispatcherServlet. (DispatcherServlet is a Spring MVC component that maps HTTP endpoints to	https://spring.io/security/cve-2023-34035	A-VMW-SPRI-020823/623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			methods on @Controller-annotated classes.) Specifically, an application is vulnerable when all of the following are true: * Spring MVC is on the classpath * Spring Security is securing more than one servlet in a single application (one of them being Spring MVC's DispatcherServlet) * The application uses requestMatchers(String) to refer to endpoints that are not Spring MVC endpoints An application is not vulnerable if any of the following is true: * The application does not have Spring MVC on the classpath * The application secures no servlets other than Spring MVC's DispatcherServlet * The application uses requestMatchers(String) only for Spring MVC endpoints **CVE ID : CVE-2023-34035**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: weaver					
Product: e-cology					
Affected Version(s): * Up to (excluding) 10.58.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jul-2023	9.8	A vulnerability was found in Weaver e-cology. It has been rated as critical. This issue affects some unknown processing of the file filelFileDownloadForOutDoc.class of the component HTTP POST Request Handler. The manipulation of the argument fileid with the input 1+WAITFOR+DELAY leads to sql injection. Upgrading to version 10.58.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-235061 was assigned to this vulnerability. **CVE ID : CVE-2023-3793**	N/A	A-WEA-E-CO-020823/624
Product: e-office					
Affected Version(s): * Up to (excluding) 9.5					
Unrestricted Upload of File with Dangerous Type	25-Jul-2023	9.8	An arbitrary file upload vulnerability in eoffice before v9.5 allows attackers to execute arbitrary code via uploading a crafted file.	N/A	A-WEA-E-OF-020823/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34798		
Vendor: webboss					
Product: webboss.io_cms					
Affected Version(s): * Up to (excluding) 3.7.0.1					
Incorrect Authorization	21-Jul-2023	7.5	An access control issue in WebBoss.io CMS v3.7.0.1 allows attackers to access the Website Backup Tool via a crafted GET request. **CVE ID : CVE-2023-36339**	N/A	A-WEB-WEBB-020823/626
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-2023	6.1	WebBoss.io CMS before v3.7.0.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2023-37742**	https://webboss.io/page/bughunter-acknowledgments.html	A-WEB-WEBB-020823/627
Vendor: webile_wifi_pc_file_transfer_project					
Product: webile_wifi_pc_file_transfer					
Affected Version(s): 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	5.4	A vulnerability was found in Webile 1.0.1. It has been classified as problematic. Affected is an unknown function of the component HTTP POST Request Handler. The manipulation of the argument new_file_name/c leads to cross site scripting. It is possible to launch	N/A	A-WEB-WEBI-020823/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the attack remotely. The exploit has been disclosed to the public and may be used. VDB-235050 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-3783**		
Vendor: webtoffee					
Product: import_export_wordpress_users					
Affected Version(s): * Up to (including) 2.4.1					
Incorrect Authorization	18-Jul-2023	7.2	The Export and Import Users and Customers plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'hf_update_customer' function called via an AJAX action in versions up to, and including, 2.4.1. This makes it possible for authenticated attackers, with shop manager-level permissions to change user passwords and potentially take over administrator accounts. **CVE ID : CVE-2023-3459**	https://plugins.trac.wordpress.org/changeset/2938705/users-customers-import-export-for-wp-woocommerce#file201, https://plugins.trac.wordpress.org/browser/users-customers-import-export-for-wp-woocommerce/tags/2.4.1/admin/modules/user/import/import.php#L446	A-WEB-IMPO-020823/629
Vendor: weintek					
Product: weincloud					
Affected Version(s): 0.13.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	19-Jul-2023	8.8	Weintek Weincloud v0.13.6 could allow an attacker to abuse the registration functionality to login with testing credentials to the official website. **CVE ID : CVE-2023-37362**	N/A	A-WEI-WEIN-020823/630
Improper Restriction of Excessive Authentication Attempts	19-Jul-2023	7.5	Weintek Weincloud v0.13.6 could allow an attacker to efficiently develop a brute force attack on credentials with authentication hints from error message responses. **CVE ID : CVE-2023-32657**	N/A	A-WEI-WEIN-020823/631
N/A	19-Jul-2023	7.5	Weintek Weincloud v0.13.6 could allow an attacker to cause a denial-of-service condition for Weincloud by sending a forged JWT token. **CVE ID : CVE-2023-34429**	N/A	A-WEI-WEIN-020823/632
Weak Password Recovery Mechanism for Forgotten Password	19-Jul-2023	5.9	Weintek Weincloud v0.13.6 could allow an attacker to reset a password with the corresponding	N/A	A-WEI-WEIN-020823/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account's JWT token only. **CVE ID : CVE-2023-35134**		
Vendor: wesecur					
Product: wesecur					
Affected Version(s): * Up to (including) 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WeSecur Security plugin <= 1.2.1 versions. **CVE ID : CVE-2023-24390**	N/A	A-WES-WESE-020823/634
Vendor: wifi_file_explorer_project					
Product: wifi_file_explorer					
Affected Version(s): 1.13.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-2023	5.4	A vulnerability was found in Dooblou WiFi File Explorer 1.13.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument search/order/download/mode leads to cross site scripting. 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-235051.	N/A	A-WIF-WIFI-020823/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3784		
Vendor: wolfcode					
Product: easyadmin8					
Affected Version(s): 2.0.2.2					
Unrestricted Upload of File with Dangerous Type	20-Jul-2023	6.6	A vulnerability was found in EasyAdmin8 2.0.2.2. It has been classified as problematic. Affected is an unknown function of the file /admin/index/index.html#/admin/mall.goods/index.html of the component File Upload Module. The manipulation leads to unrestricted upload. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235068. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-3800**	N/A	A-WOL-EASY-020823/636
Vendor: Wolfssl					
Product: wolfssl					
Affected Version(s): * Up to (excluding) 5.6.2					
Improper Certificate Validation	17-Jul-2023	8.8	If a TLS 1.3 client gets neither a PSK (pre shared key) extension	https://www.wolfssl.com/docs/sec	A-WOL-WOLF-020823/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nor a KSE (key share extension) when connecting to a malicious server, a default predictable buffer gets used for the IKM (Input Keying Material) value when generating the session master secret. Using a potentially known IKM value when generating the session master secret key compromises the key generated, allowing an eavesdropper to reconstruct it and potentially allowing access to or meddling with message contents in the session. This issue does not affect client validation of connected servers, nor expose private key information, but could result in an insecure TLS 1.3 session when not controlling both sides of the connection. wolfSSL recommends that TLS 1.3 client side users update the version of wolfSSL used. **CVE ID : CVE-2023-3724**	urity-vulnerabilities/, https://github.com/wolfSSL/wolfssl/pull/6412	
Vendor: Woocommerce					
Product: automatewoo					
Affected Version(s): * Up to (including) 5.7.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce AutomateWoo plugin <= 5.7.5 versions. **CVE ID : CVE-2023-36513**	N/A	A-WOO-AUTO-020823/638
Product: brands					
Affected Version(s): * Up to (excluding) 1.6.50					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Brands plugin <= 1.6.49 versions. **CVE ID : CVE-2023-35880**	N/A	A-WOO-BRAN-020823/639
Product: shipping_multiple_addresses					
Affected Version(s): * Up to (including) 3.8.5					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce Shipping Multiple Addresses plugin <= 3.8.5 versions. **CVE ID : CVE-2023-36514**	N/A	A-WOO-SHIP-020823/640
Product: woocommerce_order_barcodes					
Affected Version(s): * Up to (including) 1.6.4					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Order Barcodes plugin <= 1.6.4 versions.	N/A	A-WOO-WOOC-020823/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-36511		
Vendor: wpadmin					
Product: aws_cdn					
Affected Version(s): * Up to (including) 2.0.13					
Cross-Site Request Forgery (CSRF)	18-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WPAdmin WPAdmin AWS CDN plugin <= 2.0.13 versions. **CVE ID : CVE-2023-37889**	N/A	A-WPA-AWS_-020823/642
Vendor: wpdeveloper					
Product: essential_addons_for_elementor					
Affected Version(s): * Up to (including) 5.8.1					
Exposure of Sensitive Information to an Unauthorized Actor	20-Jul-2023	5.3	The Essential Addons For Elementor plugin for WordPress is vulnerable to unauthenticated API key disclosure in versions up to, and including, 5.8.1 due to the plugin adding the API key to the source code of any page running the MailChimp block. This makes it possible for unauthenticated attackers to obtain a site's MailChimp API key. We recommend resetting any MailChimp API keys if running a vulnerable version of this plugin with the MailChimp block enabled as the API key may have	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2938177%40essential-addons-for-elementor-lite&new=2938177%40essential-addons-for-elementor-lite&sfp_email=&sfph_mail=	A-WPD-ESSE-020823/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been compromised. This only affects sites running the premium version of the plugin and that have the Mailchimp block enabled on a page. **CVE ID : CVE-2023-3779**		
Vendor: wpexperts					
Product: post_smtp_mailer					
Affected Version(s): * Up to (excluding) 2.5.7					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	The POST SMTP Mailer WordPress plugin before 2.5.7 does not have proper CSRF checks in some AJAX actions, which could allow attackers to make logged in users with the manage_postman_smtp capability resend an email to an arbitrary address (for example a password reset email could be resent to an attacker controlled email, and allow them to take over an account). **CVE ID : CVE-2023-3179**	N/A	A-WPE-POST-020823/644
Product: wp_pdf_generator					
Affected Version(s): * Up to (excluding) 1.2.3					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in wpexperts.Io WP PDF Generator plugin <= 1.2.2 versions.	N/A	A-WPE-WP_P-020823/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35038		
Vendor: wpxpo					
Product: postx					
Affected Version(s): * Up to (including) 2.9.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Jul-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in wpxpo PostX – Gutenberg Post Grid Blocks plugin <= 2.9.9 versions. **CVE ID : CVE-2023-36385**	N/A	A-WPX-POST-020823/646
Vendor: wp_reroute_email_project					
Product: wp_reroute_email					
Affected Version(s): * Up to (including) 1.4.6					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Sajjad Hossain WP Reroute Email plugin <= 1.4.6 versions. **CVE ID : CVE-2023-27606**	N/A	A-WP_-WP_R-020823/647
Vendor: wp_social_autoconnect_project					
Product: wp_social_autoconnect					
Affected Version(s): * Up to (excluding) 4.6.2					
Cross-Site Request Forgery (CSRF)	17-Jul-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Justin Klein WP Social AutoConnect plugin <= 4.6.1 versions. **CVE ID : CVE-2023-37974**	N/A	A-WP_-WP_S-020823/648
Vendor: xhttp_project					
Product: xhttp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Double Free	18-Jul-2023	7.5	xHTTP 72f812d has a double free in close_connection in xhttp.c via a malformed HTTP request method. **CVE ID : CVE-2023-38434**	N/A	A-XHT-XHTT-020823/649
Vendor: yarpp					
Product: yet_another_related_posts_plugin					
Affected Version(s): * Up to (including) 5.30.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jul-2023	5.4	The YARPP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'className' parameter in versions up to, and including, 5.30.3 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2433**	https://plugins.trac.wordpress.org/changeset/2939617/yet-another-related-posts-plugin/trunk/classes/YARPP_Core.php, https://plugins.trac.wordpress.org/browser/yet-another-related-posts-plugin/tags/5.30.3/classes/YARPP_Core.php#L1623	A-YAR-YET_-020823/650
Vendor: yuque					
Product: rapidcms					
Affected Version(s): * Up to (including) 1.3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	23-Jul-2023	7.2	A vulnerability was found in OpenRapid RapidCMS up to 1.3.1. It has been declared as critical. This vulnerability affects unknown code of the file /admin/upload.php. 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. The name of the patch is 4dff387283060961c362d50105ff8da8ea40bcbe. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-235204. **CVE ID : CVE-2023-3852**	https://github.com/OpenRapid/rapidcms/commit/4dff387283060961c362d50105ff8da8ea40bcbe	A-YUQ-RAPI-020823/651
Hardware					
Vendor: aures					
Product: komet					
Affected Version(s): -					
N/A	20-Jul-2023	6.8	A vulnerability classified as problematic has been found in Aures Komet up to 20230509. This affects an unknown part of the component Kiosk Mode. The manipulation leads to	N/A	H-AUR-KOME-030823/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper access controls. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. The identifier VDB-235053 was assigned to this vulnerability. **CVE ID : CVE-2023-3786**		
Vendor: Crestron					
Product: cp3-gv_6506034					
Affected Version(s): -					
N/A	17-Jul-2023	7.5	On Crestron 3-Series Control Systems before 1.8001.0187, crafting and sending a specific BACnet packet can cause a crash. **CVE ID : CVE-2023-38405**	N/A	H-CRE-CP3--030823/653
Product: cp3n_6505417					
Affected Version(s): -					
N/A	17-Jul-2023	7.5	On Crestron 3-Series Control Systems before 1.8001.0187, crafting and sending a specific BACnet packet can cause a crash. **CVE ID : CVE-2023-38405**	N/A	H-CRE-CP3N-030823/654
Product: cp3_6504877					
Affected Version(s): -					
N/A	17-Jul-2023	7.5	On Crestron 3-Series Control Systems before 1.8001.0187, crafting and sending a	N/A	H-CRE-CP3_-030823/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific BACnet packet can cause a crash. **CVE ID : CVE-2023-38405**		
Vendor: cuby					
Product: lt400					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	Cudy LT400 1.13.4 is vulnerable to Cross Site Scripting (XSS) in cgi-bin/luci/admin/network/wireless/config via the iface parameter. **CVE ID : CVE-2023-31852**	N/A	H-CUB-LT40-030823/656
Vendor: cudy					
Product: lt400					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	Cudy LT400 1.13.4 is has a cross-site scripting (XSS) vulnerability in /cgi-bin/luci/admin/network/wireless/status via the iface parameter. **CVE ID : CVE-2023-31851**	N/A	H-CUD-LT40-030823/657
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	Cudy LT400 1.13.4 is vulnerable Cross Site Scripting (XSS) in /cgi-bin/luci/admin/network/bandwidth via the icon parameter. **CVE ID : CVE-2023-31853**	N/A	H-CUD-LT40-030823/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Dell					
Product: latitude_3420					
Affected Version(s): -					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/659
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/661
Product: latitude_3440					
Affected Version(s): -					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/663
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/664
Product: latitude_5440					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/665
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-LATI-030823/666
Insertion of Sensitive Informatio	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208	https://www.dell.com/support/kbdoc/en-	H-DEL-LATI-030823/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			(9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**	us/000215864/dsa-2023-247	
Product: optiplex_3000_thin_client					
Affected Version(s): -					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-OPTI-030823/668
Insertion of Sensitive Informatio	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306	https://www.dell.com/support/kbdo	H-DEL-OPTI-030823/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			(9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	c/en-us/000215864/dsa-2023-247	
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-OPTI-030823/670
Product: optiplex_5400					
Affected Version(s): -					
Insertion of Sensitive Informatio	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a	https://www.dell.com/support/kbdoc/en-	H-DEL-OPTI-030823/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	us/000215864/dsa-2023-247	
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-OPTI-030823/672
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-OPTI-030823/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**		
Product: wyse_3040_thin_client					
Affected Version(s): -					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/674
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**		
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/676
Product: wyse_5070_thin_client					
Affected Version(s): -					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**		
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/678
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information written to the log files. **CVE ID : CVE-2023-32455**		
Product: wyse_5470_all-in-one_thin_client					
Affected Version(s): -					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/680
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information written to the log files. **CVE ID : CVE-2023-32447**		
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/682
Product: wyse_5470_mobile_thin_client					
Affected Version(s): -					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information written to the log files. **CVE ID : CVE-2023-32446**		
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/684
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files.	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	H-DEL-WYSE-030823/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32455		
Vendor: Dlink					
Product: dir-619l					
Affected Version(s): b1					
Out-of-bounds Write	17-Jul-2023	9.8	D-Link DIR-619L v2.04(TW) was discovered to contain a stack overflow via the curTime parameter at /goform/formLogin. **CVE ID : CVE-2023-37791**	N/A	H-DLI-DIR--030823/686
Product: dir-815					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jul-2023	7.5	D-LINK DIR-815 v1.01 was discovered to contain a buffer overflow via the component /web/captcha.cgi. **CVE ID : CVE-2023-37758**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--030823/687
Vendor: espressif					
Product: esp-eye					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Con	H-ESP-ESP--030823/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	cerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-d0wd-v3					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Product: esp32-d0wdr2-v3					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/690
Product: esp32-devkitc					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/691
Product: esp32-devkitm-1					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%	H-ESP-ESP3-030823/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-mini-1					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Product: esp32-mini-1u					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/694
Product: esp32-pico-d4					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0	https://www.espressif.com/sites/def	H-ESP-ESP3-030823/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	ault/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-pico-kit					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash	H-ESP-ESP3-030823/696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-pico-mini-02					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Product: esp32-pico-mini-02u					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/698
Product: esp32-pico-v3					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM)	https://www.espressif.com/sites/default/files/ad	H-ESP-ESP3-030823/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	visory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-pico-v3-02					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encrypti	H-ESP-ESP3-030823/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	on%20Using%20EMFI%20EN.pdf	
Product: esp32-pico-v3-zero					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code.	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35818		
Product: esp32-pico-v3-zero-devkit					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/702
Product: esp32-u4wdh					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-	H-ESP-ESP3-030823/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-vaquita-dspg					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using	H-ESP-ESP3-030823/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	%20EMFI%20EN.pdf	
Product: esp32-wroom-32e					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/705
Product: esp32-wroom-32ue					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/706
Product: esp32-wroom-da					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Con	H-ESP-ESP3-030823/707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	cerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-wrover-e					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Product: esp32-wrover-ie					
Affected Version(s): -					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	H-ESP-ESP3-030823/709
Vendor: Geovision					
Product: gv-adr2701					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	19-Jul-2023	9.8	In GeoVision GV-ADR2701 cameras, an attacker could edit the login response to access the web application. **CVE ID : CVE-2023-3638**	N/A	H-GEO-GV-A-030823/710
Vendor: HP					
Product: color_laserjet_pro_4201-4203_4ra87f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/711
Product: color_laserjet_pro_4201-4203_4ra88f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: color_laserjet_pro_4201-4203_4ra89a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746795-8746795-16/hpsbpi03855	H-HP-COLO-030823/713
Product: color_laserjet_pro_4201-4203_5hh48a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746795-8746795-16/hpsbpi03855	H-HP-COLO-030823/714
Product: color_laserjet_pro_4201-4203_5hh51a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints.	https://support.hp.com/us-en/document/ish_8746795-8746795-16/hpsbpi03855	H-HP-COLO-030823/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26301		
Product: color_laserjet_pro_4201-4203_5hh52a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/716
Product: color_laserjet_pro_4201-4203_5hh53a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/717
Product: color_laserjet_pro_4201-4203_5hh59a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with certain endpoints. **CVE ID : CVE-2023-26301**		
Product: color_laserjet_pro_mfp_4301-4303_4ra80f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/719
Product: color_laserjet_pro_mfp_4301-4303_4ra81f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/720
Product: color_laserjet_pro_mfp_4301-4303_4ra82f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information	https://support.hp.com/us-en/document/ish_8746769-8746795-	H-HP-COLO-030823/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	16/hpsbpi03855	
Product: color_laserjet_pro_mfp_4301-4303_4ra83f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/722
Product: color_laserjet_pro_mfp_4301-4303_4ra84f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/723
Product: color_laserjet_pro_mfp_4301-4303_5hh64f					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of	https://support.hp.com/us-en/documen	H-HP-COLO-030823/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	t/ish_87467 69-8746795-16/hpsbpi03 855	
Product: color_laserjet_pro_mfp_4301-4303_5hh65a					
Affected Version(s): -					
Missing Authorizati on	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://supp ort.hp.com/u s-en/documen t/ish_87467 69-8746795-16/hpsbpi03 855	H-HP-COLO-030823/725
Product: color_laserjet_pro_mfp_4301-4303_5hh66a					
Affected Version(s): -					
Missing Authorizati on	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://supp ort.hp.com/u s-en/documen t/ish_87467 69-8746795-16/hpsbpi03 855	H-HP-COLO-030823/726
Product: color_laserjet_pro_mfp_4301-4303_5hh67a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/727
Product: color_laserjet_pro_mfp_4301-4303_5hh72a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/728
Product: color_laserjet_pro_mfp_4301-4303_5hh73a					
Affected Version(s): -					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	H-HP-COLO-030823/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: kratosdefense					
Product: ngc_indoor_unit					
Affected Version(s): -					
Missing Authentication for Critical Function	18-Jul-2023	9.8	Missing Authentication for a Critical Function within the Kratos NGC Indoor Unit (IDU) before 11.4 allows remote attackers to obtain arbitrary control of the IDU/ODU system. Any attacker with layer-3 network access to the IDU can impersonate the Touch Panel Unit (TPU) within the IDU by sending crafted TCP requests to the IDU. **CVE ID : CVE-2023-36669**	https://www.kratosdefense.com/vulnerability-advisories/cve-2023-36669	H-KRA-NGC_-030823/730
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Jul-2023	9.8	A remotely exploitable command injection vulnerability was found on the Kratos NGC-IDU 9.1.0.4. An attacker can execute arbitrary Linux commands as root by sending crafted TCP requests to the device. **CVE ID : CVE-2023-36670**	https://www.kratosdefense.com/vulnerability-advisories/cve-2023-36670	H-KRA-NGC_-030823/731
Vendor: rigol					
Product: mso5000					
Affected Version(s): -					
Improper Neutralization of	16-Jul-2023	9.8	The web interface on the RIGOL MSO5000 digital oscilloscope	N/A	H-RIG-MSO5-030823/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			with firmware 00.01.03.00.03 allows remote attackers to execute arbitrary code via shell metacharacters in pass1 to the webcontrol changepwd.cgi application. **CVE ID : CVE-2023-38378**		
N/A	16-Jul-2023	7.5	The web interface on the RIGOL MSO5000 digital oscilloscope with firmware 00.01.03.00.03 allows remote attackers to change the admin password via a zero-length pass0 to the webcontrol changepwd.cgi application, i.e., the entered password only needs to match the first zero characters of the saved password. **CVE ID : CVE-2023-38379**	N/A	H-RIG-MSO5-030823/733
Vendor: Rockwellautomation					
Product: kinetix_5700					
Affected Version(s): series_a					
Uncontrolled Resource Consumption	18-Jul-2023	7.5	The Rockwell Automation Kinetix 5700 DC Bus Power Supply Series A is vulnerable to CIP fuzzing. The new	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140029	H-ROC-KINE-030823/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ENIP connections cannot be established if impacted by this vulnerability, which prohibits operational capabilities of the device resulting in a denial-of-service attack. **CVE ID : CVE-2023-2263**		
Vendor: showmojo					
Product: mojobox					
Affected Version(s): -					
Authentication Bypass by Capture-replay	20-Jul-2023	8.1	ShowMojo MojoBox Digital Lockbox 1.4 is vulnerable to Authentication Bypass. The implementation of the lock opening mechanism via Bluetooth Low Energy (BLE) is vulnerable to replay attacks. A malicious user is able to intercept BLE requests and replicate them to open the lock at any time. Alternatively, an attacker with physical access to the device on which the Android app is installed, can obtain the latest BLE messages via the app logs and use them for opening the lock. **CVE ID : CVE-2023-34625**	N/A	H-SHO-MOJO-030823/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: taphome					
Product: core					
Affected Version(s): -					
Improper Authentication	17-Jul-2023	8.8	A hidden API exists in TapHome's core platform before version 2023.2 that allows an authenticated, low privileged user to change passwords of other users without any prior knowledge. The attacker may gain full access to the device by using this vulnerability. **CVE ID : CVE-2023-2759**	N/A	H-TAP-CORE-030823/736
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2023	7.6	An SQL injection vulnerability exists in TapHome core HandleMessageUpdateDevicePropertiesRequest function before version 2023.2, allowing low privileged users to inject arbitrary SQL directives into an SQL query and execute arbitrary SQL commands and get full reading access. This may also lead to limited write access and temporary Denial-of-Service. **CVE ID : CVE-2023-2760**	N/A	H-TAP-CORE-030823/737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: totolink					
Product: cp300\+					
Affected Version(s): -					
N/A	17-Jul-2023	7.5	TOTOLINK CP300+ V5.2cu.7594 contains a Denial of Service vulnerability in function RebootSystem of the file lib/cste_modules/system which can reboot the system. **CVE ID : CVE-2023-34669**	N/A	H-TOT-CP30-030823/738
Vendor: Tp-link					
Product: archer_c20					
Affected Version(s): 1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jul-2023	7.5	TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of Service (DoS) when parsing crafted data. **CVE ID : CVE-2023-30383**	N/A	H-TP--ARCH-030823/739
Product: archer_c2_v1					
Affected Version(s): -					
Buffer Copy without	18-Jul-2023	7.5	TP-LINK Archer C50v2 Archer C50(US)_V2_160801,	N/A	H-TP--ARCH-030823/740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of Service (DoS) when parsing crafted data. **CVE ID : CVE-2023-30383**		
Product: archer_c50					
Affected Version(s): 2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jul-2023	7.5	TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of Service (DoS) when parsing crafted data. **CVE ID : CVE-2023-30383**	N/A	H-TP--ARCH-030823/741
Vendor: ui					
Product: aircube					
Affected Version(s): -					
Out-of-bounds Write	18-Jul-2023	7.5	A heap overflow vulnerability found in EdgeRouters and Aircubes allows a malicious actor to	https://community.ui.com/releases/Security-Advisory-	H-UI-AIRC-030823/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interrupt UPnP service to said devices. **CVE ID : CVE-2023-31998**	Bulletin-033-033/17f7c7c0-830b-4625-a2ee-e90e514e7b0f	
Product: edgemax_edgerouter					
Affected Version(s): -					
Out-of-bounds Write	18-Jul-2023	7.5	A heap overflow vulnerability found in EdgeRouters and Aircubes allows a malicious actor to interrupt UPnP service to said devices. **CVE ID : CVE-2023-31998**	https://community.ui.com/releases/Security-Advisory-Bulletin-033-033/17f7c7c0-830b-4625-a2ee-e90e514e7b0f	H-UI-EDGE-030823/743
Vendor: Zyxel					
Product: nxc2500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-NXC2-030823/744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-NXC2-030823/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: nxc5500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-NXC5-030823/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-NXC5-030823/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_20w-vpn					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28767		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/749
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-USG_-030823/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_2200-vpn					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/755
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	H-ZYX-USG_-030823/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/757
Improper Neutralization of	17-Jul-2023	8	A command injection vulnerability in the hotspot management	https://www.zyxel.com/global/en/s	H-ZYX-USG_-030823/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-	H-ZYX-USG_-030823/759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	firewalls-and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	H-ZYX-USG_-030823/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	and-wlan-controllers	
Product: usg_flex_100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/763
Improper Neutralization of Special Elements used in an OS	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	H-ZYX-USG_-030823/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34141		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/767
Product: usg_flex_100w					
Affected Version(s): -					
Improper Neutralization of	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input	https://www.zyxel.com/global/en/s	H-ZYX-USG_-030823/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-	H-ZYX-USG_-030823/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/771
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	H-ZYX-USG_-030823/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_flex_200					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/776
Improper Neutralization of Special Elements used in an OS	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	H-ZYX-USG_-030823/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34139		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/779
Improper Neutralization of Special Elements used in an OS	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	H-ZYX-USG_-030823/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-USG_-030823/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: usg_flex_50					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36,	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	H-ZYX-USG_-030823/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/785
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: usg_flex_500					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/789
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/z	H-ZYX-USG_-030823/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	yxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/792
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-USG_-030823/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_flex_50w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/798
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	H-ZYX-USG_-030823/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/801
Buffer Copy	17-Jul-2023	6.5	A buffer overflow vulnerability in the	https://www.zyxel.com	H-ZYX-USG_-030823/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: usg_flex_700					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-USG_-030823/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/806
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-USG_-030823/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: zywall_atp100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/811
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	H-ZYX-ZYWA-030823/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34140		
Product: zywall_atp100w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/816
Use of Externally-Controlled	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions	https://www.zyxel.com/global/en/support/secu	H-ZYX-ZYWA-030823/817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Format String			5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	rity-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/821
Product: zywall_atp200					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/822
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	H-ZYX-ZYWA-030823/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/827
Product: zywall_atp500					
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')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/828
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	H-ZYX-ZYWA-030823/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34141		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/833
Product: zywall_atp700					
Affected Version(s): -					
Improper Neutralization of	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input	https://www.zyxel.com/global/en/s	H-ZYX-ZYWA-030823/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-	H-ZYX-ZYWA-030823/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/838
Buffer Copy	17-Jul-2023	6.5	A buffer overflow vulnerability in the	https://www.zyxel.com	H-ZYX-ZYWA-030823/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: zywall_atp800					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-ZYWA-030823/840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/843
Improper Neutralization of Special Elements	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series	https://www.zyxel.com/global/en/support/security-	H-ZYX-ZYWA-030823/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	H-ZYX-ZYWA-030823/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: zywall_vpn100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	H-ZYX-ZYWA-030823/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/849
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34140		
Product: zywall_vpn2s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/853
Use of Externally-Controlled	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions	https://www.zyxel.com/global/en/support/secu	H-ZYX-ZYWA-030823/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Format String			5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	rity-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/856
Improper Neutralization of Special Elements used in an OS	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	H-ZYX-ZYWA-030823/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: zywall_vpn300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/862
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	H-ZYX-ZYWA-030823/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/865
Buffer Copy	17-Jul-2023	6.5	A buffer overflow vulnerability in the	https://www.zyxel.com	H-ZYX-ZYWA-030823/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: zywall_vpn50					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	H-ZYX-ZYWA-030823/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/870
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: zywall_vpn_100					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/875
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	H-ZYX-ZYWA-030823/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/877
Improper Neutralization of	17-Jul-2023	8	A command injection vulnerability in the hotspot management	https://www.zyxel.com/global/en/s	H-ZYX-ZYWA-030823/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-	H-ZYX-ZYWA-030823/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	firewalls-and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	H-ZYX-ZYWA-030823/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	and-wlan-controllers	
Product: zywall_vpn_300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/883
Improper Neutralization of Special Elements used in an OS	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	H-ZYX-ZYWA-030823/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34141		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/887
Product: zywall_vpn_50					
Affected Version(s): -					
Improper Neutralization of	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input	https://www.zyxel.com/global/en/s	H-ZYX-ZYWA-030823/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-	H-ZYX-ZYWA-030823/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/891
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	H-ZYX-ZYWA-030823/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	H-ZYX-ZYWA-030823/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Operating System					
Vendor: ami					
Product: megarac_sp-x					
Affected Version(s): 12					
Improper Control of Generation of Code ('Code Injection')	18-Jul-2023	8.8	AMI SPx contains a vulnerability in the BMC where a user may inject code which could be executed via a Dynamic Redfish Extension interface. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34330**	N/A	O-AMI-MEGA-030823/895
Authentication Bypass by Spoofing	18-Jul-2023	8	AMI MegaRAC SPx12 contains a vulnerability in BMC where a User may cause an authentication bypass by spoofing the HTTP header. A successful exploit of this vulnerability may lead to loss of	N/A	O-AMI-MEGA-030823/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability. **CVE ID : CVE-2023-34329**		
Affected Version(s): 13					
Improper Control of Generation of Code ('Code Injection')	18-Jul-2023	8.8	AMI SPx contains a vulnerability in the BMC where a user may inject code which could be executed via a Dynamic Redfish Extension interface. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability. **CVE ID : CVE-2023-34330**	N/A	O-AMI-MEGA-030823/897
Authentication Bypass by Spoofing	18-Jul-2023	8	AMI MegaRAC SPx12 contains a vulnerability in BMC where a User may cause an authentication bypass by spoofing the HTTP header. A successful exploit of this vulnerability may lead to loss of confidentiality, integrity, and availability.	N/A	O-AMI-MEGA-030823/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34329		
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Deserialization of Untrusted Data	17-Jul-2023	9.8	CWE-502 Deserialization of Untrusted Data at the rabbitmq-connector plugin module in Apache EventMesh (incubating) V1.7.0\V1.8.0 on windows\linux\macos e.g. platforms allows attackers to send controlled message and remote code execute via rabbitmq messages. Users can use the code under the master branch in project repo to fix this issue, we will release the new version as soon as possible. **CVE ID : CVE-2023-26512**	N/A	O-APP-MACO-030823/899
Improper Neutralization of Special Elements used in an SQL Command	19-Jul-2023	7	There is SQL injection vulnerability in Esri ArcGIS Insights Desktop for Mac and Windows version 2022.1 that may allow a local, authorized attacker to execute	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-insights-security-	O-APP-MACO-030823/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			arbitrary SQL commands against the back-end database. The effort required to generate the crafted input required to exploit this issue is complex and requires significant effort before a successful attack can be expected. **CVE ID : CVE-2023-25839**	patches-for-arcgis-insights-2022-1-are-now-available/	
Vendor: aures					
Product: komet_firmware					
Affected Version(s): * Up to (including) 20230509					
N/A	20-Jul-2023	6.8	A vulnerability classified as problematic has been found in Aures Komet up to 20230509. This affects an unknown part of the component Kiosk Mode. The manipulation leads to improper access controls. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. The identifier VDB-235053 was assigned to this vulnerability. **CVE ID : CVE-2023-3786**	N/A	O-AUR-KOME-030823/901
Vendor: Crestron					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: cp3-gv_6506034_firmware					
Affected Version(s): * Up to (excluding) 1.8001.0187					
N/A	17-Jul-2023	7.5	On Crestron 3-Series Control Systems before 1.8001.0187, crafting and sending a specific BACnet packet can cause a crash. **CVE ID : CVE-2023-38405**	N/A	O-CRE-CP3--030823/902
Product: cp3n_6505417_firmware					
Affected Version(s): * Up to (excluding) 1.8001.0187					
N/A	17-Jul-2023	7.5	On Crestron 3-Series Control Systems before 1.8001.0187, crafting and sending a specific BACnet packet can cause a crash. **CVE ID : CVE-2023-38405**	N/A	O-CRE-CP3N-030823/903
Product: cp3_6504877_firmware					
Affected Version(s): * Up to (excluding) 1.8001.0187					
N/A	17-Jul-2023	7.5	On Crestron 3-Series Control Systems before 1.8001.0187, crafting and sending a specific BACnet packet can cause a crash. **CVE ID : CVE-2023-38405**	N/A	O-CRE-CP3_-030823/904
Vendor: cuby					
Product: lt400_firmware					
Affected Version(s): 1.13.4					
Improper Neutralization of Input During Web Page	17-Jul-2023	6.1	Cudy LT400 1.13.4 is vulnerable to Cross Site Scripting (XSS) in cgi-bin/luci/admin/network/wireless/config	N/A	O-CUB-LT40-030823/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			via the iface parameter. **CVE ID : CVE-2023-31852**		
Vendor: cudy					
Product: lt400_firmware					
Affected Version(s): 1.13.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	Cudy LT400 1.13.4 is has a cross-site scripting (XSS) vulnerability in /cgi-bin/luci/admin/network/wireless/status via the iface parameter. **CVE ID : CVE-2023-31851**	N/A	O-CUD-LT40-030823/906
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	Cudy LT400 1.13.4 is vulnerable Cross Site Scripting (XSS) in /cgi-bin/luci/admin/network/bandwidth via the icon parameter. **CVE ID : CVE-2023-31853**	N/A	O-CUD-LT40-030823/907
Affected Version(s): 1.15.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-2023	6.1	Cudy LT400 1.13.4 is has a cross-site scripting (XSS) vulnerability in /cgi-bin/luci/admin/network/wireless/status via the iface parameter. **CVE ID : CVE-2023-31851**	N/A	O-CUD-LT40-030823/908
Affected Version(s): 1.15.27					
Improper Neutralizat	17-Jul-2023	6.1	Cudy LT400 1.13.4 is has a cross-site	N/A	O-CUD-LT40-030823/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			scripting (XSS) vulnerability in /cgi-bin/luci/admin/network/wireless/status via the iface parameter. **CVE ID : CVE-2023-31851**		
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Integer Overflow or Wraparound	17-Jul-2023	5.5	iperf3 before 3.14 allows peers to cause an integer overflow and heap corruption via a crafted length field. **CVE ID : CVE-2023-38403**	https://github.com/esnet/iperf/commit/0ef151550d96cc4460f98832df84b4a1e87c65e9, https://github.com/esnet/iperf/issues/1542, https://downloads.es.net/pub/iperf/esnet-secadv-2023-0001.txt.asc	O-DEB-DEBI-030823/910
Affected Version(s): 11.0					
Use After Free	21-Jul-2023	7.8	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Flaw in the error handling of bound	https://kernel.dance/4bedf9eee016286c835e3d8fa981ddece5338795, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit	O-DEB-DEBI-030823/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chains causes a use-after-free in the abort path of NFT_MSG_NEWRULE. The vulnerability requires CAP_NET_ADMIN to be triggered. We recommend upgrading past commit 4bedf9eee016286c835e3d8fa981ddece5338795. **CVE ID : CVE-2023-3610**	?id=4bedf9eee016286c835e3d8fa981ddece5338795	
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf,	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts).		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Affected Version(s): 12.0					
N/A	18-Jul-2023	5.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK executes to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2023-22041**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle Java SE (component: Utility). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2023-22036**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22044**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2023-22045**		
N/A	18-Jul-2023	3.7	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22049**		
N/A	18-Jul-2023	3.1	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpujul2023.html	O-DEB-DEBI-030823/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2023-22006**		
Vendor: Dell					
Product: powerstoreos					
Affected Version(s): * Up to (excluding) 3.5.0.1					
Insertion of Sensitive	21-Jul-2023	4.9		https://www.dell.com/s	O-DEL-POWE-030823/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			Dell PowerStore versions prior to 3.5.0.1 contain an insertion of sensitive information into log file vulnerability. A high privileged malicious user could potentially exploit this vulnerability, leading to sensitive information disclosure. **CVE ID : CVE-2023-32478**	upport/kbdoc/en-us/000215171/dsa-2023-173-dell-powerstore-family-security-update-for-multiple-vulnerabilities	
Product: wyse_thinos					
Affected Version(s): * Up to (excluding) 9.4.2103					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2306 (9.4.2103) contain a sensitive information disclosure vulnerability. A malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32447**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	O-DEL-WYSE-030823/925
Affected Version(s): * Up to (including) 9.3.2102					
Insertion of Sensitive	20-Jul-2023	5.5		https://www.dell.com/s	O-DEL-WYSE-030823/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information into Log File			Dell Wyse ThinOS versions prior to 2208 (9.3.2102) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32455**	upport/kbdoc/en-us/000215864/dsa-2023-247	
Affected Version(s): 9.4.1141					
Insertion of Sensitive Information into Log File	20-Jul-2023	5.5	Dell Wyse ThinOS versions prior to 2303 (9.4.1141) contain a sensitive information disclosure vulnerability. An unauthenticated malicious user with local access to the device could exploit this vulnerability to read sensitive information written to the log files. **CVE ID : CVE-2023-32446**	https://www.dell.com/support/kbdoc/en-us/000215864/dsa-2023-247	O-DEL-WYSE-030823/927
Vendor: Dlink					
Product: dir-619l_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.04					
Out-of-bounds Write	17-Jul-2023	9.8	D-Link DIR-619L v2.04(TW) was discovered to contain a stack overflow via the curTime parameter at /goform/formLogin. **CVE ID : CVE-2023-37791**	N/A	O-DLI-DIR--030823/928
Product: dir-815_firmware					
Affected Version(s): 1.0.1					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jul-2023	7.5	D-LINK DIR-815 v1.01 was discovered to contain a buffer overflow via the component /web/captcha.cgi. **CVE ID : CVE-2023-37758**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--030823/929
Vendor: espressif					
Product: esp-eye_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using	O-ESP-ESP--030823/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP--030823/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: esp32-d0wd-v3_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/932
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Con	O-ESP-ESP3-030823/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	cerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-d0wdr2-v3_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/935
Product: esp32-devkitc_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0	https://www.espressif.com/sites/def	O-ESP-ESP3-030823/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	ault/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encrypti	O-ESP-ESP3-030823/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	on%20Using%20EMFI%20EN.pdf	
Product: esp32-devkitm-1_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code.	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35818		
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/939
Product: esp32-mini-1u_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Secu	O-ESP-ESP3-030823/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	rity%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Product: esp32-mini-1_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/942
Affected Version(s): 3.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/943
Product: esp32-pico-d4_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%	O-ESP-ESP3-030823/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Product: esp32-pico-kit_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/946
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3	https://www.espressif.com/sites/default/files/advisory_downloads/AR202	O-ESP-ESP3-030823/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	3-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-pico-mini-02u_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using	O-ESP-ESP3-030823/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/949
Product: esp32-pico-mini-02_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/950
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%	O-ESP-ESP3-030823/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-pico-v3-02_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/953
Product: esp32-pico-v3-zero-devkit_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI	https://www.espressif.com/sites/default/files/advisory_down	O-ESP-ESP3-030823/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	loads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using	O-ESP-ESP3-030823/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	%20EMFI%20EN.pdf	
Product: esp32-pico-v3-zero_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/957
Product: esp32-pico-v3_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Con	O-ESP-ESP3-030823/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	cerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Product: esp32-u4wdh_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/960
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM)	https://www.espressif.com/sites/default/files/ad	O-ESP-ESP3-030823/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	visory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-vaquita-dspg_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encrypti	O-ESP-ESP3-030823/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	on%20Using%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code.	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35818		
Product: esp32-wroom-32e_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/964
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Secu	O-ESP-ESP3-030823/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	rity%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-wroom-32ue_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode.	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/967
Product: esp32-wroom-da_firmware					
Affected Version(s): 3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/968
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%2	O-ESP-ESP3-030823/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	0Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Product: esp32-wrover-e_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/971
Product: esp32-wrover-ie_firmware					
Affected Version(s): 3.0					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3	https://www.espressif.com/sites/default/files/advisory_downloads/AR202	O-ESP-ESP3-030823/972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**	3-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	
Affected Version(s): 3.1					
N/A	17-Jul-2023	6.8	An issue was discovered on Espressif ESP32 3.0 (ESP32_rev300 ROM) devices. An EMFI attack on ECO3 provides the attacker with a capability to influence the PC value at the CPU context level, regardless of Secure Boot and Flash Encryption status. By using this capability, the attacker can exploit another behavior in the chip to gain unauthorized access to the ROM	https://www.espressif.com/sites/default/files/advisory_downloads/AR2023-005%20Security%20Advisory%20Concerning%20Bypassing%20Secure%20Boot%20and%20Flash%20Encryption%20Using%20EMFI%20EN.pdf	O-ESP-ESP3-030823/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			download mode. Access to ROM download mode may be further exploited to read the encrypted flash content in cleartext format or execute stub code. **CVE ID : CVE-2023-35818**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 37					
Unquoted Search Path or Element	20-Jul-2023	9.8	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. **CVE ID : CVE-2023-38408**	https://github.com/openbsd/src/commit/7bc29a9d5cd697290aa056e94ecee6253d3425f8, https://www.openssh.com/txt/release-9.3p2, https://news.ycombinator.com/item?id=36790196, https://github.com/openbsd/src/commit/f8f5a6b003981bb824329dc987d101977beda7ca	O-FED-FEDO-030823/974
Affected Version(s): 38					
Unquoted Search	20-Jul-2023	9.8	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2	https://github.com/openbsd/src/com	O-FED-FEDO-030823/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path or Element			has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. **CVE ID : CVE-2023-38408**	mit/7bc29a9d5cd697290aa056e94ecee6253d3425f8, https://www.openssh.com/txt/release-9.3p2, https://news.ycombinator.com/item?id=36790196, https://github.com/openbsd/src/commit/f8f5a6b003981bb824329dc987d101977beda7ca	
Loop with Unreachable Exit Condition ('Infinite Loop')	20-Jul-2023	7.5	An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows	https://www.samba.org/samba/security/CVE-2023-34966	O-FED-FEDO-030823/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial of service condition. **CVE ID : CVE-2023-34966**		
N/A	20-Jul-2023	5.9	A vulnerability was found in Samba's SMB2 packet signing mechanism. The SMB2 packet signing is not enforced if an admin configured "server signing = required" or for SMB2 connections to Domain Controllers where SMB2 packet signing is mandatory. This flaw allows an attacker to perform attacks, such as a man-in-the-middle attack, by intercepting the network traffic and modifying the SMB2 messages between client and server, affecting the integrity of the data. **CVE ID : CVE-2023-3347**	https://www.samba.org/samba/security/CVE-2023-3347.html	O-FED-FEDO-030823/977
Improper Locking	18-Jul-2023	5.5	A deadlock flaw was found in the Linux kernel's BPF subsystem. This flaw allows a local user to potentially crash the system. **CVE ID : CVE-2023-0160**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ed17aa92dc56, https://lore.kernel.org/al	O-FED-FEDO-030823/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				l/CABcoxUaayum5oOqFMMqAeWuS8+EzojquSOSyDA3J_2omY=2EeAg@mail.gmail.com/	
Access of Resource Using Incompatible Type ('Type Confusion')	20-Jul-2023	5.3	A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the mdssvc protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc	https://www.samba.org/samba/security/CVE-2023-34967.html	O-FED-FEDO-030823/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			worker process, affecting all other clients this worker serves. **CVE ID : CVE-2023-34967**		
N/A	20-Jul-2023	5.3	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path. **CVE ID : CVE-2023-34968**	https://www.samba.org/samba/security/CVE-2023-34968.html	O-FED-FEDO-030823/980
N/A	19-Jul-2023	2.8	A flaw was found in the keylime attestation verifier, which fails to flag a device's submitted TPM quote as faulty when the quote's signature does not validate for some reason. Instead, it will only emit an error in the log without flagging the device as untrusted. **CVE ID : CVE-2023-3674**	https://bugzilla.redhat.com/show_bug.cgi?id=2222903, https://github.com/keylime/keylime/commit/95ce3d86bd2c53009108ffda2dcf553312d733db	O-FED-FEDO-030823/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Geovision					
Product: gv-adr2701_firmware					
Affected Version(s): 1.00_2017_12_15					
Improper Authentication	19-Jul-2023	9.8	In GeoVision GV-ADR2701 cameras, an attacker could edit the login response to access the web application. **CVE ID : CVE-2023-3638**	N/A	O-GEO-GV-A-030823/982
Vendor: HP					
Product: color_laserjet_pro_4201-4203_4ra87f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/983
Product: color_laserjet_pro_4201-4203_4ra88f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with certain endpoints. **CVE ID : CVE-2023-26301**		
Product: color_laserjet_pro_4201-4203_4ra89a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/985
Product: color_laserjet_pro_4201-4203_5hh48a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/986
Product: color_laserjet_pro_4201-4203_5hh51a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information	https://support.hp.com/us-en/document/ish_8746769-8746795-	O-HP-COLO-030823/987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	16/hpsbpi03855	
Product: color_laserjet_pro_4201-4203_5hh52a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/988
Product: color_laserjet_pro_4201-4203_5hh53a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/989
Product: color_laserjet_pro_4201-4203_5hh59a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of	https://support.hp.com/us-en/documen	O-HP-COLO-030823/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	t/ish_87467 69-8746795-16/hpsbpi03 855	
Product: color_laserjet_pro_mfp_4301-4303_4ra80f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorizati on	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://supp ort.hp.com/u s-en/documen t/ish_87467 69-8746795-16/hpsbpi03 855	O-HP-COLO-030823/991
Product: color_laserjet_pro_mfp_4301-4303_4ra81f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorizati on	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://supp ort.hp.com/u s-en/documen t/ish_87467 69-8746795-16/hpsbpi03 855	O-HP-COLO-030823/992
Product: color_laserjet_pro_mfp_4301-4303_4ra82f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/993
Product: color_laserjet_pro_mfp_4301-4303_4ra83f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/994
Product: color_laserjet_pro_mfp_4301-4303_4ra84f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: color_laserjet_pro_mfp_4301-4303_5hh64f_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746795-8746795-16/hpsbpi03855	O-HP-COLO-030823/996
Product: color_laserjet_pro_mfp_4301-4303_5hh65a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746795-8746795-16/hpsbpi03855	O-HP-COLO-030823/997
Product: color_laserjet_pro_mfp_4301-4303_5hh66a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints.	https://support.hp.com/us-en/document/ish_8746795-8746795-16/hpsbpi03855	O-HP-COLO-030823/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26301		
Product: color_laserjet_pro_mfp_4301-4303_5hh67a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/999
Product: color_laserjet_pro_mfp_4301-4303_5hh72a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication with certain endpoints. **CVE ID : CVE-2023-26301**	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/1000
Product: color_laserjet_pro_mfp_4301-4303_5hh73a_firmware					
Affected Version(s): * Up to (excluding) 6.12.1.12-202306030312					
Missing Authorization	21-Jul-2023	9.8	Certain HP LaserJet Pro print products are potentially vulnerable to an Elevation of Privilege and/or Information Disclosure related to a lack of authentication	https://support.hp.com/us-en/document/ish_8746769-8746795-16/hpsbpi03855	O-HP-COLO-030823/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with certain endpoints. **CVE ID : CVE-2023-26301**		
Product: hp-ux					
Affected Version(s): -					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	O-HP-HP-U-030823/1002
Vendor: IBM					
Product: aix					
Affected Version(s): -					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	O-IBM-AIX-030823/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Jul-2023	6.7	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 with a Federated configuration is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user with SYSADM privileges could overflow the buffer and execute arbitrary code on the system. IBM X-Force ID: 257763. **CVE ID : CVE-2023-35012**	https://www.ibm.com/support/pages/node/7010747, https://exchange.xforce.ibmcloud.com/vulnerabilities/257763	O-IBM-AIX-030823/1004
N/A	19-Jul-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information due to an insecure security configuration in InfoSphere Data Flow Designer. IBM X-Force ID: 259352. **CVE ID : CVE-2023-35898**	https://www.ibm.com/support/pages/node/7009205, https://exchange.xforce.ibmcloud.com/vulnerabilities/259352	O-IBM-AIX-030823/1005
Server-Side Request Forgery (SSRF)	19-Jul-2023	5.4	IBM Sterling Connect:Express for UNIX 1.5 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	https://www.ibm.com/support/pages/node/7010923, https://exchange.xforce.ibmcloud.com/vulnerabi	O-IBM-AIX-030823/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enumeration or facilitating other attacks. IBM X-Force ID: 252135. **CVE ID : CVE-2023-29260**	lities/252135	
N/A	19-Jul-2023	5.3	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055. **CVE ID : CVE-2023-29259**	https://exchange.xforce.ibmcloud.com/vulnerabilities/252055, https://www.ibm.com/support/pages/node/7010921	O-IBM-AIX-030823/1007
N/A	17-Jul-2023	5.3	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain system information using a specially crafted query that could aid in further attacks against the system. IBM X-Force ID: 257695. **CVE ID : CVE-2023-33857**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257695, https://www.ibm.com/support/pages/node/7007059	O-IBM-AIX-030823/1008
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Jul-2023	4.7	IBM Spectrum Protect 8.1.0.0 through 8.1.17.0 could allow a local user to cause a denial of service due to due to improper time-of-check to time-of-use functionality. IBM X-Force ID: 256012.	https://exchange.xforce.ibmcloud.com/vulnerabilities/256012, https://www.ibm.com/support/pages/node/7011761	O-IBM-AIX-030823/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33832		
Product: i					
Affected Version(s): -					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	O-IBM-I-030823/1010
Product: linux_on_ibm_z					
Affected Version(s): -					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	O-IBM-LINU-030823/1011
Vendor: icewhale					
Product: casaos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 0.4.4					
Missing Authentication for Critical Function	17-Jul-2023	9.8	CasaOS is an open-source Personal Cloud system. Due to a lack of IP address verification an unauthenticated attackers can execute arbitrary commands as `root` on CasaOS instances. The problem was addressed by improving the detection of client IP addresses in `391dd7f`. This patch is part of CasaOS 0.4.4. Users should upgrade to CasaOS 0.4.4. If they can't, they should temporarily restrict access to CasaOS to untrusted users, for instance by not exposing it publicly. **CVE ID : CVE-2023-37265**	https://github.com/IceWhaleTech/CasaOS-Gateway/security/advisories/GHSA-vjh7-5r6x-xh6g, https://github.com/IceWhaleTech/CasaOS-Gateway/commit/391dd7f0f239020c46bf057cfa25f82031fc15f7	O-ICE-CASA-030823/1012
Improper Authentication	17-Jul-2023	9.8	CasaOS is an open-source Personal Cloud system. Unauthenticated attackers can craft arbitrary JWTs and access features that usually require authentication and execute arbitrary commands as `root` on CasaOS instances. This problem was addressed by improving the	https://github.com/IceWhaleTech/CasaOS/security/advisories/GHSA-m5q5-8mfw-p2hr, https://github.com/IceWhaleTech/CasaOS/commit/705bf1facbffd2ca40b15	O-ICE-CASA-030823/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of JWTs in commit `705bf1f`. This patch is part of CasaOS 0.4.4. Users should upgrade to CasaOS 0.4.4. If they can't, they should temporarily restrict access to CasaOS to untrusted users, for instance by not exposing it publicly. **CVE ID : CVE-2023-37266**	9b0303132b6fdf657ad	
Affected Version(s): 0.4.4					
Missing Authentication for Critical Function	17-Jul-2023	9.8	CasaOS is an open-source Personal Cloud system. Due to a lack of IP address verification an unauthenticated attackers can execute arbitrary commands as `root` on CasaOS instances. The problem was addressed by improving the detection of client IP addresses in `391dd7f`. This patch is part of CasaOS 0.4.4. Users should upgrade to CasaOS 0.4.4. If they can't, they should temporarily restrict access to CasaOS to untrusted users, for instance by not exposing it publicly. **CVE ID : CVE-2023-37265**	https://github.com/IceWhaleTech/CasaOS-Gateway/security/advisories/GHSA-vjh7-5r6x-xh6g, https://github.com/IceWhaleTech/CasaOS-Gateway/commit/391dd7f0f239020c46bf057cfa25f82031fc15f7	O-ICE-CASA-030823/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: kratosdefense					
Product: ngc_indoor_unit_firmware					
Affected Version(s): * Up to (excluding) 11.4					
Missing Authentication for Critical Function	18-Jul-2023	9.8	Missing Authentication for a Critical Function within the Kratos NGC Indoor Unit (IDU) before 11.4 allows remote attackers to obtain arbitrary control of the IDU/ODU system. Any attacker with layer-3 network access to the IDU can impersonate the Touch Panel Unit (TPU) within the IDU by sending crafted TCP requests to the IDU. **CVE ID : CVE-2023-36669**	https://www.kratosdefense.com/vulnerability-advisories/cve-2023-36669	O-KRA-NGC_-030823/1015
Affected Version(s): 9.1.0.4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Jul-2023	9.8	A remotely exploitable command injection vulnerability was found on the Kratos NGC-IDU 9.1.0.4. An attacker can execute arbitrary Linux commands as root by sending crafted TCP requests to the device. **CVE ID : CVE-2023-36670**	https://www.kratosdefense.com/vulnerability-advisories/cve-2023-36670	O-KRA-NGC_-030823/1016
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	17-Jul-2023	9.8	CWE-502 Deserialization of Untrusted Data at the rabbitmq-connector plugin module in Apache EventMesh (incubating) V1.7.0\V 1.8.0 on windows\linux\mac os e.g. platforms allows attackers to send controlled message and remote code execute via rabbitmq messages. Users can use the code under the master branch in project repo to fix this issue, we will release the new version as soon as possible. **CVE ID : CVE-2023-26512**	N/A	O-LIN-LINU-030823/1017
Improper Certificate Validation	18-Jul-2023	8.1	Improper Validation of Certificate with Host Mismatch vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Man in the Middle Attack.This issue affects Hitachi Device Manager: before 8.8.5-02.	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-125/index.html	O-LIN-LINU-030823/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34143		
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	O-LIN-LINU-030823/1019
Cleartext Transmission of Sensitive Information	18-Jul-2023	7.5	Cleartext Transmission of Sensitive Information vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Interception.This issue affects Hitachi Device Manager: before 8.8.5-02. **CVE ID : CVE-2023-34142**	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-125/index.html	O-LIN-LINU-030823/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Double Free	18-Jul-2023	7.5	xHTTP 72f812d has a double free in close_connection in xhttp.c via a malformed HTTP request method. **CVE ID : CVE-2023-38434**	N/A	O-LIN-LINU-030823/1021
Out-of-bounds Write	17-Jul-2023	6.7	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 with a Federated configuration is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user with SYSADM privileges could overflow the buffer and execute arbitrary code on the system. IBM X-Force ID: 257763. **CVE ID : CVE-2023-35012**	https://www.ibm.com/support/pages/node/7010747, https://exchange.xforce.ibmcloud.com/vulnerabilities/257763	O-LIN-LINU-030823/1022
N/A	19-Jul-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information due to an insecure security configuration in InfoSphere Data Flow Designer. IBM X-Force ID: 259352. **CVE ID : CVE-2023-35898**	https://www.ibm.com/support/pages/node/7009205, https://exchange.xforce.ibmcloud.com/vulnerabilities/259352	O-LIN-LINU-030823/1023
Integer Overflow	17-Jul-2023	5.5	iperf3 before 3.14 allows peers to cause	https://github.com/esnet	O-LIN-LINU-030823/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			an integer overflow and heap corruption via a crafted length field. **CVE ID : CVE-2023-38403**	/iperf/commit/0ef151550d96cc4460f98832df84b4a1e87c65e9, https://github.com/esnet/iperf/issues/1542, https://downloads.es.net/pub/iperf/esnet-secadv-2023-0001.txt.asc	
Server-Side Request Forgery (SSRF)	19-Jul-2023	5.4	IBM Sterling Connect:Express for UNIX 1.5 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: 252135. **CVE ID : CVE-2023-29260**	https://www.ibm.com/support/pages/node/7010923, https://exchange.xforce.ibmcloud.com/vulnerabilities/252135	O-LIN-LINU-030823/1025
N/A	19-Jul-2023	5.3	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055.	https://exchange.xforce.ibmcloud.com/vulnerabilities/252055, https://www.ibm.com/support/page	O-LIN-LINU-030823/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29259	s/node/7010921	
N/A	17-Jul-2023	5.3	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain system information using a specially crafted query that could aid in further attacks against the system. IBM X-Force ID: 257695. **CVE ID : CVE-2023-33857**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257695, https://www.ibm.com/support/pages/node/7007059	O-LIN-LINU-030823/1027
Time-of-check Time-of-use (TOCTOU) Race Condition	19-Jul-2023	4.7	IBM Spectrum Protect 8.1.0.0 through 8.1.17.0 could allow a local user to cause a denial of service due to due to improper time-of-check to time-of-use functionality. IBM X-Force ID: 256012. **CVE ID : CVE-2023-33832**	https://exchange.xforce.ibmcloud.com/vulnerabilities/256012, https://www.ibm.com/support/pages/node/7011761	O-LIN-LINU-030823/1028
Affected Version(s): * Up to (excluding) 6.2.12					
N/A	17-Jul-2023	5.5	An issue was discovered in set_con2fb_map in drivers/video/fbdev/core/fbcon.c in the Linux kernel before 6.2.12. Because an assignment occurs only for the first vc, the fbcon_registered_fb and fbcon_display arrays can be desynchronized in	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=fffb0b52d5258554c645c966c6cbef7de50b851d	O-LIN-LINU-030823/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fbcon_mode_deleted (the con2fb_map points at the old fb_info). **CVE ID : CVE-2023-38409**		
Affected Version(s): * Up to (excluding) 6.3.10					
Out-of-bounds Read	18-Jul-2023	9.1	An issue was discovered in the Linux kernel before 6.3.10. fs/smb/server/smb2misc.c in ksmbd does not validate the relationship between the command payload size and the RFC1002 length specification, leading to an out-of-bounds read. **CVE ID : CVE-2023-38432**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/smb/server?id=2b9b8f3b68edb3d67d79962f02e26dbb5ae3808d	O-LIN-LINU-030823/1030
Affected Version(s): * Up to (excluding) 6.3.4					
Off-by-one Error	18-Jul-2023	9.8	An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/connection.c in ksmbd has an off-by-one error in memory allocation (because of ksmbd_smb2_check_message) that may lead to out-of-bounds access. **CVE ID : CVE-2023-38429**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/ksmbd?id=443d61d1fa9faa60ef925513d83742902390100f	O-LIN-LINU-030823/1031
Out-of-bounds Read	18-Jul-2023	9.1	An issue was discovered in the Linux kernel before	https://git.kernel.org/pub/scm/linux	O-LIN-LINU-030823/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.3.4. ksmbd has an out-of-bounds read in smb2_find_context_vals when create_context's name_len is larger than the tag length. **CVE ID : CVE-2023-38426**	/kernel/git/torvalds/linux.git/commit/fs/ksmbd?id=02f76c401d17e409ed45bf7887148fcc22c93c85	
Out-of-bounds Read	18-Jul-2023	9.1	An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/smb2pdu.c in ksmbd does not properly check the UserName value because it does not consider the address of security buffer, leading to an out-of-bounds read. **CVE ID : CVE-2023-38428**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/ksmbd?id=f0a96d1aafd8964e1f9955c830a3e5cb3c60a90f	O-LIN-LINU-030823/1033
Affected Version(s): * Up to (excluding) 6.3.8					
Out-of-bounds Read	18-Jul-2023	9.8	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/smb2pdu.c in ksmbd has an integer underflow and out-of-bounds read in deassemble_neg_contexts. **CVE ID : CVE-2023-38427**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/smb/server?id=f1a411873c85b642f13b01f21b534c2bab81fc1b	O-LIN-LINU-030823/1034
Out-of-bounds Read	18-Jul-2023	9.1	An issue was discovered in the Linux kernel before 6.3.8. fs/smb/server/conne	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linu	O-LIN-LINU-030823/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ction.c in ksmbd does not validate the relationship between the NetBIOS header's length field and the SMB header sizes, via pdu_size in ksmbd_conn_handler_loop, leading to an out-of-bounds read. **CVE ID : CVE-2023-38431**	x.git/commit/fs/smb/server?id=368ba06881c395f1c9a7ba22203cf8d78b4addc0	
Affected Version(s): * Up to (excluding) 6.3.9					
Out-of-bounds Read	18-Jul-2023	9.1	An issue was discovered in the Linux kernel before 6.3.9. ksmbd does not validate the SMB request protocol ID, leading to an out-of-bounds read. **CVE ID : CVE-2023-38430**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/fs/smb/server?id=1c1bcf2d3ea061613119b534f57507c377df20f9	O-LIN-LINU-030823/1036
Affected Version(s): * Up to (excluding) 6.4					
Improper Locking	18-Jul-2023	5.5	A deadlock flaw was found in the Linux kernel's BPF subsystem. This flaw allows a local user to potentially crash the system. **CVE ID : CVE-2023-0160**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ed17aa92dc56, https://lore.kernel.org/all/CABcoxUaym5oOqFMMqAeWuS8+EzojquSOSyDA3J_2omY=	O-LIN-LINU-030823/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2EeAg@mail.gmail.com/	
Affected Version(s): 6.4					
Use After Free	21-Jul-2023	7.8	A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, u32_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 04c55383fa5689357bcdd2c8036725a55ed632bc. **CVE ID : CVE-2023-3609**	https://kernel.dance/04c55383fa5689357bcdd2c8036725a55ed632bc, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=04c55383fa5689357bcdd2c8036725a55ed632bc	O-LIN-LINU-030823/1038
Use After Free	21-Jul-2023	7.8	A use-after-free vulnerability in the Linux kernel's	https://kernel.dance/4bedf9eee01628	O-LIN-LINU-030823/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netfilter: nf_tables component can be exploited to achieve local privilege escalation. Flaw in the error handling of bound chains causes a use-after-free in the abort path of NFT_MSG_NEWRULE. The vulnerability requires CAP_NET_ADMIN to be triggered. We recommend upgrading past commit 4bedf9eee016286c835e3d8fa981ddece5338795. **CVE ID : CVE-2023-3610**	6c835e3d8fa981ddece5338795, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=4bedf9eee016286c835e3d8fa981ddece5338795	
Affected Version(s): 6.5					
Out-of-bounds Write	21-Jul-2023	7.8	An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The qfq_change_agg() function in net/sched/sch_qfq.c	https://kernel.dance/3e337087c3b5805fe0b8a46ba622a962880b5d64, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3e3370	O-LIN-LINU-030823/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows an out-of-bounds write because lmax is updated according to packet sizes without bounds checks. We recommend upgrading past commit 3e337087c3b5805fe0b8a46ba622a962880b5d64. **CVE ID : CVE-2023-3611**	87c3b5805fe0b8a46ba622a962880b5d64	
Use After Free	21-Jul-2023	7.8	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, fw_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=0323bce598eea038714f941ce2b22541c46d488f, https://kernel.dance/0323bce598eea038714f941ce2b22541c46d488f	O-LIN-LINU-030823/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We recommend upgrading past commit 0323bce598eea038714f941ce2b22541c46d488f. **CVE ID : CVE-2023-3776**		
Affected Version(s): From (including) 2.6 Up to (excluding) 6.5					
Use After Free	21-Jul-2023	7.8	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, fw_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 0323bce598eea03871	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=0323bce598eea038714f941ce2b22541c46d488f, https://kernel.dance/0323bce598eea038714f941ce2b22541c46d488f	O-LIN-LINU-030823/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4f941ce2b22541c46d488f. **CVE ID : CVE-2023-3776**		
Affected Version(s): From (including) 3.8 Up to (excluding) 6.5					
Out-of-bounds Write	21-Jul-2023	7.8	An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The qfq_change_agg() function in net/sched/sch_qfq.c allows an out-of-bounds write because lmax is updated according to packet sizes without bounds checks. We recommend upgrading past commit 3e337087c3b5805fe0b8a46ba622a962880b5d64. **CVE ID : CVE-2023-3611**	https://kernel.dance/3e337087c3b5805fe0b8a46ba622a962880b5d64, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3e337087c3b5805fe0b8a46ba622a962880b5d64	O-LIN-LINU-030823/1043
Affected Version(s): From (including) 4.14 Up to (excluding) 6.4					
Use After Free	21-Jul-2023	7.8	A use-after-free vulnerability in the	https://kernel.dance/04c	O-LIN-LINU-030823/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, u32_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 04c55383fa5689357bcdd2c8036725a55ed632bc. **CVE ID : CVE-2023-3609**	55383fa5689357bcdd2c8036725a55ed632bc, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=04c55383fa5689357bcdd2c8036725a55ed632bc	
Affected Version(s): From (including) 5.9 Up to (excluding) 6.4					
Use After Free	21-Jul-2023	7.8	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve	https://kernel.dance/4bedf9eee016286c835e3d8fa981ddece5338795, https://git.k	O-LIN-LINU-030823/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local privilege escalation. Flaw in the error handling of bound chains causes a use-after-free in the abort path of NFT_MSG_NEWRULE. The vulnerability requires CAP_NET_ADMIN to be triggered. We recommend upgrading past commit 4bedf9eee016286c835e3d8fa981ddece5338795. **CVE ID : CVE-2023-3610**	ernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=4bedf9eee016286c835e3d8fa981ddece5338795	
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Deserialization of Untrusted Data	17-Jul-2023	9.8	CWE-502 Deserialization of Untrusted Data at the rabbitmq-connector plugin module in Apache EventMesh (incubating) V1.7.0\V1.8.0 on windows\linux\macos e.g. platforms allows attackers to	N/A	O-MIC-WIND-030823/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			send controlled message and remote code execute via rabbitmq messages. Users can use the code under the master branch in project repo to fix this issue, we will release the new version as soon as possible. **CVE ID : CVE-2023-26512**		
Improper Certificate Validation	18-Jul-2023	8.1	Improper Validation of Certificate with Host Mismatch vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Man in the Middle Attack.This issue affects Hitachi Device Manager: before 8.8.5-02. **CVE ID : CVE-2023-34143**	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-125/index.html	O-MIC-WIND-030823/1047
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations,	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/s	O-MIC-WIND-030823/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	upport/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	
Cleartext Transmission of Sensitive Information	18-Jul-2023	7.5	Cleartext Transmission of Sensitive Information vulnerability in Hitachi Device Manager on Windows, Linux (Device Manager Server, Device Manager Agent, Host Data Collector components) allows Interception.This issue affects Hitachi Device Manager: before 8.8.5-02. **CVE ID : CVE-2023-34142**	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-125/index.html	O-MIC-WIND-030823/1049
Out-of-bounds Write	21-Jul-2023	7.5	An out-of-bounds write vulnerability on windows operating systems causes the Ivanti AntiVirus Product to crash. Update to Ivanti AV Product version 7.9.1.285 or above. **CVE ID : CVE-2023-35077**	https://forums.ivanti.com/s/article/SA-2023-07-19-CVE-2023-35077	O-MIC-WIND-030823/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Jul-2023	7	There is SQL injection vulnerability in Esri ArcGIS Insights Desktop for Mac and Windows version 2022.1 that may allow a local, authorized attacker to execute arbitrary SQL commands against the back-end database. The effort required to generate the crafted input required to exploit this issue is complex and requires significant effort before a successful attack can be expected. **CVE ID : CVE-2023-25839**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-insights-security-patches-for-arcgis-insights-2022-1-are-now-available/	O-MIC-WIND-030823/1051
Out-of-bounds Write	17-Jul-2023	6.7	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 with a Federated configuration is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local user with SYSADM privileges could overflow the buffer and execute arbitrary code on the system. IBM X-Force ID: 257763.	https://www.ibm.com/support/pages/node/7010747, https://exchange.xforce.ibmcloud.com/vulnerabilities/257763	O-MIC-WIND-030823/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35012		
N/A	19-Jul-2023	6.5	IBM InfoSphere Information Server 11.7 could allow an authenticated user to obtain sensitive information due to an insecure security configuration in InfoSphere Data Flow Designer. IBM X-Force ID: 259352. **CVE ID : CVE-2023-35898**	https://www.ibm.com/support/pages/node/7009205, https://exchange.xforce.ibmcloud.com/vulnerabilities/259352	O-MIC-WIND-030823/1053
Server-Side Request Forgery (SSRF)	19-Jul-2023	5.4	IBM Sterling Connect:Express for UNIX 1.5 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: 252135. **CVE ID : CVE-2023-29260**	https://www.ibm.com/support/pages/node/7010923, https://exchange.xforce.ibmcloud.com/vulnerabilities/252135	O-MIC-WIND-030823/1054
N/A	19-Jul-2023	5.3	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055.	https://exchange.xforce.ibmcloud.com/vulnerabilities/252055, https://www.ibm.com/support/page	O-MIC-WIND-030823/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29259	s/node/7010921	
N/A	17-Jul-2023	5.3	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain system information using a specially crafted query that could aid in further attacks against the system. IBM X-Force ID: 257695. **CVE ID : CVE-2023-33857**	https://exchange.xforce.ibmcloud.com/vulnerabilities/257695, https://www.ibm.com/support/pages/node/7007059	O-MIC-WIND-030823/1056
N/A	19-Jul-2023	5.3	IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.4 and 23.0.0 through 23.0.5 is vulnerable to disclosing server version information which may be used to determine software vulnerabilities at the operating system level. IBM X-Force ID: 259368. **CVE ID : CVE-2023-35900**	https://exchange.xforce.ibmcloud.com/vulnerabilities/259368, https://www.ibm.com/support/pages/node/7010895	O-MIC-WIND-030823/1057
Improper Authentication	17-Jul-2023	5.3	IBM Robotic Process Automation 21.0.0 through 21.0.7.6 and 23.0.0 through 23.0.6 is vulnerable to client side validation bypass which could allow invalid changes or values in some fields. IBM X-Force ID: 259380.	https://exchange.xforce.ibmcloud.com/vulnerabilities/259380, https://www.ibm.com/support/pages/node/7012317	O-MIC-WIND-030823/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35901		
Absolute Path Traversal	19-Jul-2023	10	Absolute Path Traversal in GitHub repository mlflow/mlflow prior to 2.5.0. **CVE ID : CVE-2023-3765**	https://github.com/mlflow/mlflow/commit/6dde93758d42455cb90ef324407919ed67668b9b, https://huntr.dev/bounties/4be5fd63-8a0a-490d-9ee1-f33dc768ed76	O-MIC-WIND-030823/1059
Vendor: Mikrotik					
Product: routeros					
Affected Version(s): * Up to (including) 6.48.7					
N/A	19-Jul-2023	7.2	MikroTik RouterOS stable before 6.49.7 and long-term through 6.48.6 are vulnerable to a privilege escalation issue. A remote and authenticated attacker can escalate privileges from admin to super-admin on the Winbox or HTTP interface. The attacker can abuse this vulnerability to execute arbitrary code on the system. **CVE ID : CVE-2023-30799**	N/A	O-MIK-ROUT-030823/1060
Affected Version(s): From (including) 6.34 Up to (excluding) 6.49.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Jul-2023	7.2	MikroTik RouterOS stable before 6.49.7 and long-term through 6.48.6 are vulnerable to a privilege escalation issue. A remote and authenticated attacker can escalate privileges from admin to super-admin on the Winbox or HTTP interface. The attacker can abuse this vulnerability to execute arbitrary code on the system. **CVE ID : CVE-2023-30799**	N/A	O-MIK-ROUT-030823/1061
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
N/A	19-Jul-2023	7.5	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.3 CD and IBM MQ Appliance 9.2 LTS, 9.3 LTS, 9.2 CD, and 9.2 LTS, under certain configurations, is vulnerable to a denial of service attack caused by an error processing messages. IBM X-Force ID: 250397. **CVE ID : CVE-2023-28513**	https://www.ibm.com/support/pages/node/7007731, https://www.ibm.com/support/pages/node/7007421, https://exchange.xforce.ibmcloud.com/vulnerabilities/250397	O-ORA-SOLA-030823/1062
Server-Side	19-Jul-2023	5.4	IBM Sterling Connect:Express for	https://www.ibm.com/s	O-ORA-SOLA-030823/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			UNIX 1.5 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: 252135. **CVE ID : CVE-2023-29260**	upport/pages/node/7010923, https://exchange.xforce.ibmcloud.com/vulnerabilities/252135	
N/A	19-Jul-2023	5.3	IBM Sterling Connect:Express for UNIX 1.5 browser UI is vulnerable to attacks that rely on the use of cookies without the SameSite attribute. IBM X-Force ID: 252055. **CVE ID : CVE-2023-29259**	https://exchange.xforce.ibmcloud.com/vulnerabilities/252055, https://www.ibm.com/support/pages/node/7010921	O-ORA-SOLA-030823/1064
Affected Version(s): 11					
N/A	18-Jul-2023	7.8	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device Driver Interface). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle	https://www.oracle.com/security-alerts/cpujul2023.html	O-ORA-SOLA-030823/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. Note: CVE-2023-22023 is equivalent to CVE-2023-31284. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2023-22023**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	20-Jul-2023	7.5	An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100%	https://www.samba.org/samba/security/CVE-2023-34966	O-RED-ENTE-030823/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial of service condition. **CVE ID : CVE-2023-34966**		
N/A	20-Jul-2023	5.9	A vulnerability was found in Samba's SMB2 packet signing mechanism. The SMB2 packet signing is not enforced if an admin configured "server signing = required" or for SMB2 connections to Domain Controllers where SMB2 packet signing is mandatory. This flaw allows an attacker to perform attacks, such as a man-in-the-middle attack, by intercepting the network traffic and modifying the SMB2 messages between client and server, affecting the integrity of the data. **CVE ID : CVE-2023-3347**	https://www.samba.org/samba/security/CVE-2023-3347.html	O-RED-ENTE-030823/1067
Access of Resource Using Incompatible Type ('Type Confusion')	20-Jul-2023	5.3	A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-	https://www.samba.org/samba/security/CVE-2023-34967.html	O-RED-ENTE-030823/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			value style dictionary where the keys are character strings, and the values can be any of the supported types in the mdssvc protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc worker process, affecting all other clients this worker serves. **CVE ID : CVE-2023-34967**		
N/A	20-Jul-2023	5.3	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the	https://www.samba.org/samba/security/CVE-2023-34968.html	O-RED-ENTE-030823/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path. **CVE ID : CVE-2023-34968**		
Affected Version(s): 9.0					
Loop with Unreachable Exit Condition ('Infinite Loop')	20-Jul-2023	7.5	An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial of service condition. **CVE ID : CVE-2023-34966**	https://www.samba.org/samba/security/CVE-2023-34966	O-RED-ENTE-030823/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Jul-2023	5.9	A vulnerability was found in Samba's SMB2 packet signing mechanism. The SMB2 packet signing is not enforced if an admin configured "server signing = required" or for SMB2 connections to Domain Controllers where SMB2 packet signing is mandatory. This flaw allows an attacker to perform attacks, such as a man-in-the-middle attack, by intercepting the network traffic and modifying the SMB2 messages between client and server, affecting the integrity of the data. **CVE ID : CVE-2023-3347**	https://www.samba.org/samba/security/CVE-2023-3347.html	O-RED-ENTE-030823/1071
Access of Resource Using Incompatible Type ('Type Confusion')	20-Jul-2023	5.3	A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the mdssvc protocol. Due to a lack of type checking in callers of the	https://www.samba.org/samba/security/CVE-2023-34967.html	O-RED-ENTE-030823/1072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc worker process, affecting all other clients this worker serves. **CVE ID : CVE-2023-34967**		
N/A	20-Jul-2023	5.3	A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path.	https://www.samba.org/samba/security/CVE-2023-34968.html	O-RED-ENTE-030823/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34968		
Vendor: rigol					
Product: mso5000_firmware					
Affected Version(s): 00.01.03.00.03					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jul-2023	9.8	The web interface on the RIGOL MSO5000 digital oscilloscope with firmware 00.01.03.00.03 allows remote attackers to execute arbitrary code via shell metacharacters in pass1 to the webcontrol changepwd.cgi application. **CVE ID : CVE-2023-38378**	N/A	O-RIG-MSO5-030823/1074
N/A	16-Jul-2023	7.5	The web interface on the RIGOL MSO5000 digital oscilloscope with firmware 00.01.03.00.03 allows remote attackers to change the admin password via a zero-length pass0 to the webcontrol changepwd.cgi application, i.e., the entered password only needs to match the first zero characters of the saved password. **CVE ID : CVE-2023-38379**	N/A	O-RIG-MSO5-030823/1075
Vendor: Rockwellautomation					
Product: kinetix_5700_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 13.001					
Uncontrolled Resource Consumption	18-Jul-2023	7.5	The Rockwell Automation Kinetix 5700 DC Bus Power Supply Series A is vulnerable to CIP fuzzing. The new ENIP connections cannot be established if impacted by this vulnerability, which prohibits operational capabilities of the device resulting in a denial-of-service attack. **CVE ID : CVE-2023-2263**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140029	O-ROC-KINE-030823/1076
Vendor: showmojo					
Product: mojobox_firmware					
Affected Version(s): 1.4					
Authentication Bypass by Capture-replay	20-Jul-2023	8.1	ShowMojo MojoBox Digital Lockbox 1.4 is vulnerable to Authentication Bypass. The implementation of the lock opening mechanism via Bluetooth Low Energy (BLE) is vulnerable to replay attacks. A malicious user is able to intercept BLE requests and replicate them to open the lock at any time.	N/A	O-SHO-MOJO-030823/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Alternatively, an attacker with physical access to the device on which the Android app is installed, can obtain the latest BLE messages via the app logs and use them for opening the lock. **CVE ID : CVE-2023-34625**		
Vendor: taphome					
Product: core_firmware					
Affected Version(s): * Up to (excluding) 2023.2					
Improper Authentication	17-Jul-2023	8.8	A hidden API exists in TapHome's core platform before version 2023.2 that allows an authenticated, low privileged user to change passwords of other users without any prior knowledge. The attacker may gain full access to the device by using this vulnerability. **CVE ID : CVE-2023-2759**	N/A	O-TAP-CORE-030823/1078
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-2023	7.6	An SQL injection vulnerability exists in TapHome core HandleMessageUpdateDevicePropertiesRequest function before version 2023.2, allowing low privileged users to inject arbitrary SQL directives into an SQL query and execute	N/A	O-TAP-CORE-030823/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary SQL commands and get full reading access. This may also lead to limited write access and temporary Denial-of-Service. **CVE ID : CVE-2023-2760**		
Vendor: totolink					
Product: cp300\+_firmware					
Affected Version(s): 5.2cu.7594					
N/A	17-Jul-2023	7.5	TOTOLINK CP300+ V5.2cu.7594 contains a Denial of Service vulnerability in function RebootSystem of the file lib/cste_modules/system which can reboot the system. **CVE ID : CVE-2023-34669**	N/A	O-TOT-CP30-030823/1080
Vendor: Tp-link					
Product: archer_c20_firmware					
Affected Version(s): 150707					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jul-2023	7.5	TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of	N/A	O-TP--ARCH-030823/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) when parsing crafted data. **CVE ID : CVE-2023-30383**		
Product: archer_c2_v1_firmware					
Affected Version(s): 170228					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jul-2023	7.5	TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of Service (DoS) when parsing crafted data. **CVE ID : CVE-2023-30383**	N/A	O-TP--ARCH-030823/1082
Product: archer_c50_firmware					
Affected Version(s): 160801					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jul-2023	7.5	TP-LINK Archer C50v2 Archer C50(US)_V2_160801, TP-LINK Archer C20v1 Archer_C20_V1_150707, and TP-LINK Archer C2v1 Archer_C2_US__V1_170228 were discovered to contain a buffer overflow which may lead to a Denial of Service (DoS) when parsing crafted data.	N/A	O-TP--ARCH-030823/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30383		
Vendor: ui					
Product: aircube_firmware					
Affected Version(s): * Up to (excluding) 2.8.9					
Out-of-bounds Write	18-Jul-2023	7.5	A heap overflow vulnerability found in EdgeRouters and Aircubes allows a malicious actor to interrupt UPnP service to said devices. **CVE ID : CVE-2023-31998**	https://community.ui.com/releases/Security-Advisory-Bulletin-033-033/17f7c7c0-830b-4625-a2ee-e90e514e7b0f	O-UI-AIRC-030823/1084
Product: edgemax_edgerouter_firmware					
Affected Version(s): 2.0.9					
Out-of-bounds Write	18-Jul-2023	7.5	A heap overflow vulnerability found in EdgeRouters and Aircubes allows a malicious actor to interrupt UPnP service to said devices. **CVE ID : CVE-2023-31998**	https://community.ui.com/releases/Security-Advisory-Bulletin-033-033/17f7c7c0-830b-4625-a2ee-e90e514e7b0f	O-UI-EDGE-030823/1085
Vendor: Zyxel					
Product: nxc2500_firmware					
Affected Version(s): From (including) 6.10\\(aaig.0\\) Up to (including) 6.10\\(aaig.3\\)					
Improper Neutralization of Special Elements used in an	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions	https://www.zyxel.com/global/en/support/security-advisories/z	O-ZYX-NXC2-030823/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	yxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	O-ZYX-NXC2-030823/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: nxc5500_firmware					
Affected Version(s): From (including) 6.10\\(aaos.0\\) Up to (including) 6.10\\(aaos.4\\)					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	O-ZYX-NXC5-030823/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-NXC5-030823/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_20w-vpn_firmware					
Affected Version(s): From (including) 4.16 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 5.10 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1093
Use of Externally-Controlled	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series	https://www.zyxel.com/global/en/s	O-ZYX-USG_-030823/1094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Format String			firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	O-ZYX-USG_-030823/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	and-wlan-controllers	
Product: usg_2200-vpn_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1098
Improper Neutralization of Special Elements used in an OS	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	O-ZYX-USG_-030823/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34139		
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1102
Product: usg_flex_100w_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralizat	17-Jul-2023	8	A command injection vulnerability in the	https://www.zyxel.com	O-ZYX-USG_-030823/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-USG_-030823/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.50 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_flex_100_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1112
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-USG_-030823/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.50 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1115
Buffer Copy without	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series	https://www.zyxel.com/global/en/s	O-ZYX-USG_-030823/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: usg_flex_200_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-	O-ZYX-USG_-030823/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1120
Improper Neutralization of Special	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature	https://www.zyxel.com/global/en/support/secu	O-ZYX-USG_-030823/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	rity-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 4.50 Up to (excluding) 5.37					
Improper Neutralization of Special Elements	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series	https://www.zyxel.com/global/en/support/security-	O-ZYX-USG_-030823/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_flex_500_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1125
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	O-ZYX-USG_-030823/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.50 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1129
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-USG_-030823/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	vulnerabilities-in-firewalls-and-wlan-controllers	
Product: usg_flex_50w_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1134
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-USG_-030823/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	es-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 4.50 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-	O-ZYX-USG_-030823/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	firewalls-and-wlan-controllers	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: usg_flex_50_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1138
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions	https://www.zyxel.com/global/en/support/security-	O-ZYX-USG_-030823/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-	O-ZYX-USG_-030823/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.50 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1143
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: usg_flex_700_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1147
Improper Neutralization of Special Elements used in an OS	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX	https://www.zyxel.com/global/en/support/security-advisories/zyxel-	O-ZYX-USG_-030823/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.50 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-34139		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-USG_-030823/1151
Product: zywall_atp100w_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of	17-Jul-2023	8	A command injection vulnerability in the hotspot management	https://www.zyxel.com/global/en/s	O-ZYX-ZYWA-030823/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	upport/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	es-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-	O-ZYX-ZYWA-030823/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Affected Version(s): From (including) 4.32 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1157
Product: zywall_atp100_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralizat	17-Jul-2023	8	A command injection vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-ZYWA-030823/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	es-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Affected Version(s): From (including) 4.32 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1163
Product: zywall_atp200_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralizat	17-Jul-2023	8	A command injection vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-ZYWA-030823/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	es-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Affected Version(s): From (including) 4.32 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1169
Product: zywall_atp500_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralizat	17-Jul-2023	8	A command injection vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-ZYWA-030823/1171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	es-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Affected Version(s): From (including) 4.32 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1175
Product: zywall_atp700_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralizat	17-Jul-2023	8	A command injection vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-ZYWA-030823/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	es-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Affected Version(s): From (including) 4.32 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1181
Product: zywall_atp800_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralizat	17-Jul-2023	8	A command injection vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-ZYWA-030823/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.10 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	es-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Affected Version(s): From (including) 4.32 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1187
Product: zywall_vpn100_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralizat	17-Jul-2023	8	A command injection vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W)	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-	O-ZYX-ZYWA-030823/1189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	vulnerabilities-in-firewalls-and-wlan-controllers	
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled.	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33012		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1193
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: zywall_vpn2s_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1197
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1200
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy	17-Jul-2023	6.5	A buffer overflow vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: zywall_vpn300_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	O-ZYX-ZYWA-030823/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36,	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1206
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1207
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: zywall_vpn50_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1211
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1214
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy	17-Jul-2023	6.5	A buffer overflow vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: zywall_vpn_100_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	O-ZYX-ZYWA-030823/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36,	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1220
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1221
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		
Product: zywall_vpn_300_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**		
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1225
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabiliti	O-ZYX-ZYWA-030823/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	es-in-firewalls-and-wlan-controllers	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**		
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions 4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1228
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy	17-Jul-2023	6.5	A buffer overflow vulnerability in the	https://www.zyxel.com	O-ZYX-ZYWA-030823/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service (DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**	/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Product: zywall_vpn_50_firmware					
Affected Version(s): From (including) 4.60 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command	17-Jul-2023	8	A command injection vulnerability in the hotspot management feature of the Zyxel ATP series firmware versions 4.60 through 5.36 Patch 2, USG FLEX series firmware	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-	O-ZYX-ZYWA-030823/1230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			versions 4.60 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.60 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.60 through 5.36 Patch 2, and VPN series firmware versions 4.60 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the list of trusted RADIUS clients in advance. **CVE ID : CVE-2023-34138**	advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 5.00 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	The configuration parser fails to sanitize user-controlled input in the Zyxel ATP series firmware versions 5.10 through 5.36, USG FLEX series firmware versions 5.00 through 5.36, USG FLEX 50(W) series firmware versions 5.10 through 5.36, USG20(W)-VPN series firmware versions 5.10 through 5.36, and	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VPN series firmware versions 5.00 through 5.36. An unauthenticated, LAN-based attacker could leverage the vulnerability to inject some operating system (OS) commands into the device configuration data on an affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-28767**		
Use of Externally-Controlled Format String	17-Jul-2023	8.8	A format string vulnerability in the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted PPPoE configuration on an	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device when the cloud management mode is enabled. **CVE ID : CVE-2023-33011**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-2023	8.8	A command injection vulnerability in the configuration parser of the Zyxel ATP series firmware versions 5.10 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.10 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.10 through 5.36 Patch 2, and VPN series firmware versions 5.00 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands by using a crafted GRE configuration when the cloud management mode is enabled. **CVE ID : CVE-2023-33012**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1233
Improper Neutralization of Special Elements	17-Jul-2023	8	A command injection vulnerability in the access point (AP) management feature of the Zyxel ATP series	https://www.zyxel.com/global/en/support/security-	O-ZYX-ZYWA-030823/1234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			firmware versions 5.00 through 5.36 Patch 2, USG FLEX series firmware versions 5.00 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 5.00 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 5.00 through 5.36 Patch 2, VPN series firmware versions 5.00 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device if the attacker could trick an authorized administrator to add their IP address to the managed AP list in advance. **CVE ID : CVE-2023-34141**	advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 4.20 Up to (excluding) 5.37					
Improper Neutralization of Special Elements used in an	17-Jul-2023	8.8	A command injection vulnerability in the Free Time WiFi hotspot feature of the Zyxel USG FLEX series firmware versions	https://www.zyxel.com/global/en/support/security-advisories/z	O-ZYX-ZYWA-030823/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			4.50 through 5.36 Patch 2 and VPN series firmware versions 4.20 through 5.36 Patch 2, could allow an unauthenticated, LAN-based attacker to execute some OS commands on an affected device. **CVE ID : CVE-2023-34139**	yxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	
Affected Version(s): From (including) 4.30 Up to (excluding) 5.37					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-2023	6.5	A buffer overflow vulnerability in the Zyxel ATP series firmware versions 4.32 through 5.36 Patch 2, USG FLEX series firmware versions 4.50 through 5.36 Patch 2, USG FLEX 50(W) series firmware versions 4.16 through 5.36 Patch 2, USG20(W)-VPN series firmware versions 4.16 through 5.36 Patch 2, VPN series firmware versions 4.30 through 5.36 Patch 2, NXC2500 firmware versions 6.10(AAIG.0) through 6.10(AAIG.3), and NXC5500 firmware versions 6.10(AAOS.0) through 6.10(AAOS.4), could allow an unauthenticated, LAN-based attacker to cause denial of service	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-wlan-controllers	O-ZYX-ZYWA-030823/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(DoS) conditions by sending a crafted request to the CAPWAP daemon. **CVE ID : CVE-2023-34140**		