National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

16 – 31 Dec 2023 Vol. 10 No. 24

Table of Content

Common Vulnerabilities and Exposures (CVE) Report					
Weakness	**Publish Date**	**CVSSv3**	**Description & CVE ID**	**Patch**	**NCIIPC ID**
Application					
Vendor: 52north					
Product: wps					
Affected Version(s): * Up to (excluding) 4.0.0					
Improper Restriction of XML External Entity Reference	19-Dec-2023	7.5	An XXE (XML External Entity) vulnerability has been detected in 52North WPS affecting versions prior to 4.0.0-beta.11. This vulnerability allows the use of external entities in its WebProcessingService servlet for an attacker to retrieve files by making HTTP requests to the internal network. **CVE ID : CVE-2023-6280**	N/A	A-52N-WPS-160124/1
Affected Version(s): 4.0.0					
Improper Restriction of XML External Entity Reference	19-Dec-2023	7.5	An XXE (XML External Entity) vulnerability has been detected in 52North WPS affecting versions prior to 4.0.0-beta.11. This vulnerability allows the use of external entities in its WebProcessingService servlet for an	N/A	A-52N-WPS-160124/2

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to retrieve files by making HTTP requests to the internal network. **CVE ID : CVE-2023-6280**		
Vendor: ab-wp					
Product: simple_counter					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AB-WP Simple Counter allows Stored XSS.This issue affects Simple Counter: from n/a through 1.0.2. **CVE ID : CVE-2023-50377**	N/A	A-AB--SIMP-160124/3
Vendor: accredible					
Product: accredible_certificates_\&_open_badges					
Affected Version(s): * Up to (including) 1.4.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Accredible Accredible Certificates & Open	N/A	A-ACC-ACCR-160124/4

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Badges allows Stored XSS.This issue affects Accredible Certificates & Open Badges: from n/a through 1.4.8. **CVE ID : CVE-2023-50827**		
Vendor: adastracrypto					
Product: cryptocurrency_payment_\&_donation_box					
Affected Version(s): * Up to (excluding) 2.2.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Adastra Crypto Cryptocurrency Payment & Donation Box – Accept Payments in any Cryptocurrency on your WP Site for Free.This issue affects Cryptocurrency Payment & Donation Box – Accept Payments in any Cryptocurrency on your WP Site for Free: from n/a through 2.2.7.	N/A	A-ADA-CRYP-160124/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32128		
Vendor: aditaas					
Product: allied_digital_integrated_tool-as-a-service					
Affected Version(s): 5.1					
Improper Authentication	18-Dec-2023	9.8	The vulnerability exists in ADiTaaS (Allied Digital Integrated Tool-as-a-Service) version 5.1 due to an improper authentication vulnerability in the ADiTaaS backend API. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable platform. Successful exploitation of this vulnerability could allow the attacker to gain full access to the customers' data and completely compromise the targeted platform. **CVE ID : CVE-2023-6483**	N/A	A-ADI-ALLI-160124/6

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Adobe					
Product: experience_manager					
Affected Version(s): * Up to (excluding) 2023.11.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51457**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/7
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51458**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-51459**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/9
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51460**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51461**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/11
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-51462**		
Affected Version(s): * Up to (including) 6.5.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-51462**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/13
Affected Version(s): * Up to (including) 6.5.18.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51457**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51458**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/15
Improper Neutralization of Input During Web Page Generation	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2023-51459**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51460**	https://helpx.adobe.com/security/products/experience-manager/apsb23-72.html	A-ADO-EXPE-160124/17
Improper Neutralization of Input During Web Page	20-Dec-2023	5.4	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS)	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-160124/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2023-51461**	manager/apsb23-72.html	
Vendor: affiliatebooster					
Product: affiliate_booster					
Affected Version(s): * Up to (including) 3.0.5					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kulwant Nagi Affiliate Booster – Pros & Cons, Notice, and CTA Blocks for Affiliates.This issue affects Affiliate Booster – Pros & Cons, Notice, and CTA Blocks for Affiliates: from n/a through 3.0.5. **CVE ID : CVE-2023-49148**	N/A	A-AFF-AFFI-160124/19
Vendor: akshaymenariya					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: export_import_menus					
Affected Version(s): * Up to (including) 1.8.0					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in Akshay Menariya Export Import Menus.This issue affects Export Import Menus: from n/a through 1.8.0. **CVE ID : CVE-2023-34385**	N/A	A-AKS-EXPO-160124/20
Vendor: amadercode					
Product: dropshipping_\&_affiliation_with_amazon					
Affected Version(s): * Up to (including) 2.1.2					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in AmaderCode Lab Dropshipping & Affiliation with Amazon.This issue affects Dropshipping & Affiliation with Amazon: from n/a through 2.1.2. **CVE ID : CVE-2023-31215**	N/A	A-AMA-DROP-160124/21
Vendor: Apache					
Product: airflow					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.8.0					
Improper Access Control	21-Dec-2023	6.5	Apache Airflow, versions before 2.8.0, is affected by a vulnerability that allows an authenticated user without the variable edit permission, to update a variable. This flaw compromises the integrity of variable management, potentially leading to unauthorized data modification. Users are recommended to upgrade to 2.8.0, which fixes this issue **CVE ID : CVE-2023-50783**	https://github.com/apache/airflow/pull/33932	A-APA-AIRF-160124/22
Exposure of Resource to Wrong Sphere	21-Dec-2023	4.3	Apache Airflow, in versions prior to 2.8.0, contains a security vulnerability that allows an authenticated user with limited access to some DAGs, to craft a request that could give the user write access to various DAG resources for DAGs that the user had no access to, thus,	https://github.com/apache/airflow/pull/34366	A-APA-AIRF-160124/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabling the user to clear DAGs they shouldn't. This is a missing fix for CVE-2023-42792 in Apache Airflow 2.7.2 Users of Apache Airflow are strongly advised to upgrade to version 2.8.0 or newer to mitigate the risk associated with this vulnerability. **CVE ID : CVE-2023-48291**		
Affected Version(s): From (including) 2.6.0 Up to (including) 2.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Apache Airflow, versions 2.6.0 through 2.7.3 has a stored XSS vulnerability that allows a DAG author to add an unbounded and not-sanitized javascript in the parameter description field of the DAG. This Javascript can be executed on the client side of any of the user who looks at the tasks in the browser sandbox. While this issue does not allow to exit the browser	https://github.com/apache/airflow/pull/35460	A-APA-AIRF-160124/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandbox or manipulation of the server-side data - more than the DAG author already has, it allows to modify what the user looking at the DAG details sees in the browser - which opens up all kinds of possibilities of misleading other users. Users of Apache Airflow are recommended to upgrade to version 2.8.0 or newer to mitigate the risk associated with this vulnerability **CVE ID : CVE-2023-47265**		
Affected Version(s): From (including) 2.7.0 Up to (including) 2.7.3					
Cross-Site Request Forgery (CSRF)	21-Dec-2023	6.5	Apache Airflow, version 2.7.0 through 2.7.3, has a vulnerability that allows an attacker to trigger a DAG in a GET request without CSRF validation. As a result, it was possible for a malicious website opened in the same browser - by the user who also had	https://github.com/apache/airflow/pull/36026	A-APA-AIRF-160124/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Airflow UI opened - to trigger the execution of DAGs without the user's consent. Users are advised to upgrade to version 2.8.0 or later which is not affected **CVE ID : CVE-2023-49920**		
Product: doris					
Affected Version(s): * Up to (excluding) 2.0.3					
Incorrect Authorization	18-Dec-2023	8.2	The api /api/snapshot and /api/get_log_file would allow unauthenticated access. It could allow a DoS attack or get arbitrary files from FE node. Please upgrade to 2.0.3 to fix these issues. **CVE ID : CVE-2023-41314**	https://lists.apache.org/thread/tgvpvz3yw7zgodl1sb3sv3jbbz8t5zb4	A-APA-DORI-160124/26
Product: guacamole					
Affected Version(s): * Up to (including) 1.5.3					
Integer Overflow or Wraparound	19-Dec-2023	8.8	Apache Guacamole 1.5.3 and older do not consistently ensure that values received from a VNC server will not result in integer overflow. If a user connects to a	https://lists.apache.org/thread/23gzwftpfgtq97tj6ttmbclry53kmwv6	A-APA-GUAC-160124/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious or compromised VNC server, specially-crafted data could result in memory corruption, possibly allowing arbitrary code to be executed with the privileges of the running guacd process. Users are recommended to upgrade to version 1.5.4, which fixes this issue. **CVE ID : CVE-2023-43826**		
Product: sshd					
Affected Version(s): * Up to (including) 2.11.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627	A-APA-SSHD-160124/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before	bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: sshj					
Affected Version(s): * Up to (including) 0.37.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-APA-SSHJ-160124/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0,		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: superset					
Affected Version(s): * Up to (excluding) 2.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2023	8.8	A where_in JINJA macro allows users to specify a quote, which combined with a carefully crafted statement would allow for SQL injection in Apache Superset.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2, which fixes the issue.	https://lists.apache.org/thread/1kf481bgs3451qcz6hfhobs7xvhp8n1p	A-APA-SUPE-160124/30

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49736		
Incorrect Authorization	19-Dec-2023	6.5	An authenticated Gamma user has the ability to create a dashboard and add charts to it, this user would automatically become one of the owners of the charts allowing him to incorrectly have write permissions to these charts.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2 or 2.1.3, which fixes the issue. **CVE ID : CVE-2023-49734**	https://lists.apache.org/thread/985h6ltvtbvdoysso780kkj7x744cds5	A-APA-SUPE-160124/31
Affected Version(s): * Up to (excluding) 2.1.3					
Uncontrolled Resource Consumption	19-Dec-2023	6.5	Uncontrolled resource consumption can be triggered by authenticated attacker that uploads a malicious ZIP to	https://lists.apache.org/thread/yxbxg4wryb7cb7wyybk11l5nqy0rsrvl	A-APA-SUPE-160124/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			import database, dashboards or datasets. This vulnerability exists in Apache Superset versions up to and including 2.1.2 and versions 3.0.0, 3.0.1. **CVE ID : CVE-2023-46104**		
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.1					
Uncontrolled Resource Consumption	19-Dec-2023	6.5	Uncontrolled resource consumption can be triggered by authenticated attacker that uploads a malicious ZIP to import database, dashboards or datasets. This vulnerability exists in Apache Superset versions up to and including 2.1.2 and versions 3.0.0, 3.0.1. **CVE ID : CVE-2023-46104**	https://lists.apache.org/thread/yxbxg4wryb7cb7wyybk11l5nqy0rsrvl	A-APA-SUPE-160124/33
Affected Version(s): From (including) 3.0.0 Up to (excluding) 3.0.2					
Improper Neutralization of Special Elements used in an SQL	19-Dec-2023	8.8	A where_in JINJA macro allows users to specify a quote, which combined with a carefully crafted statement would	https://lists.apache.org/thread/1kf481bgs3451qcz6hfhobs7xvhp8n1p	A-APA-SUPE-160124/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			allow for SQL injection in Apache Superset.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2, which fixes the issue. **CVE ID : CVE-2023-49736**		
Incorrect Authorization	19-Dec-2023	6.5	An authenticated Gamma user has the ability to create a dashboard and add charts to it, this user would automatically become one of the owners of the charts allowing him to incorrectly have write permissions to these charts.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2 or 2.1.3,	https://lists.apache.org/thread/985h6ltvtbvdoysso780kkj7x744cds5	A-APA-SUPE-160124/35

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which fixes the issue. **CVE ID : CVE-2023-49734**		
Vendor: appmysite					
Product: appmysite					
Affected Version(s): * Up to (including) 3.11.0					
Exposure of Sensitive Information to an Unauthorized Actor	21-Dec-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in AppMySite AppMySite – Create an app with the Best Mobile App Builder.This issue affects AppMySite – Create an app with the Best Mobile App Builder: from n/a through 3.11.0. **CVE ID : CVE-2023-49762**	N/A	A-APP-APPM-160124/36
Vendor: Aruba					
Product: aruba_hispeed_cache					
Affected Version(s): * Up to (including) 2.0.6					
N/A	19-Dec-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Aruba.It Aruba HiSpeed Cache.This issue affects Aruba	N/A	A-ARU-ARUB-160124/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HiSpeed Cache: from n/a through 2.0.6. **CVE ID : CVE-2023-44983**		
Vendor: arulprasadj					
Product: prevent_landscape_rotation					
Affected Version(s): * Up to (including) 2.0					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Arul Prasad J Prevent Landscape Rotation.This issue affects Prevent Landscape Rotation: from n/a through 2.0. **CVE ID : CVE-2023-48772**	N/A	A-ARU-PREV-160124/38
Vendor: asyncssh_project					
Product: asyncssh					
Affected Version(s): * Up to (excluding) 2.14.2					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.	A-ASY-ASYN-160124/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through	xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: augustinfotech					
Product: woocommerce_menu_extension					
Affected Version(s): * Up to (including) 1.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in August Infotech WooCommerce Menu Extension allows Stored XSS.This issue affects	N/A	A-AUG-WOOC-160124/40

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WooCommerce Menu Extension: from n/a through 1.6.2. **CVE ID : CVE-2023-50834**		
Vendor: automad					
Product: automad					
Affected Version(s): * Up to (including) 1.10.9					
Server-Side Request Forgery (SSRF)	21-Dec-2023	8.8	A vulnerability was found in automad up to 1.10.9. It has been declared as critical. This vulnerability affects the function import of the file FileController.php. The manipulation of the argument importUrl leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-248686 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-AUT-AUTO-160124/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-7037		
Cross-Site Request Forgery (CSRF)	21-Dec-2023	6.5	A vulnerability was found in automad up to 1.10.9. It has been rated as problematic. This issue affects some unknown processing of the file /dashboard?controller=UserCollection::createUser of the component User Creation Handler. The manipulation leads to cross-site request forgery. 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-248687. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7038**	N/A	A-AUT-AUTO-160124/42
Improper Neutralization of Input During Web Page	21-Dec-2023	5.4	A vulnerability was found in automad up to 1.10.9 and classified as problematic. Affected by this	N/A	A-AUT-AUTO-160124/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			issue is some unknown functionality of the file packages\standard\templates\post.php of the component Setting Handler. The manipulation of the argument sitename leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248684. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7035**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	A vulnerability was found in automad up to 1.10.9. It has been classified as problematic. This affects the function upload of the file FileCollectionController.php of the component Content Type Handler. The manipulation leads to unrestricted	N/A	A-AUT-AUTO-160124/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248685 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7036**		
Vendor: Automattic					
Product: canada_post_shipping_method					
Affected Version(s): * Up to (excluding) 2.8.4					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce Canada Post Shipping Method.This issue affects Canada Post Shipping Method: from n/a through 2.8.3. **CVE ID : CVE-2023-47789**	N/A	A-AUT-CANA-160124/45
Product: woocommerce_bookings					
Affected Version(s): * Up to (excluding) 2.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Bookings.This issue affects WooCommerce Bookings: from n/a through 2.0.3. **CVE ID : CVE-2023-47787**	N/A	A-AUT-WOOC-160124/46
Affected Version(s): * Up to (including) 1.15.78					
Authorization Bypass Through User-Controlled Key	21-Dec-2023	7.5	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce WooCommerce Bookings.This issue affects WooCommerce Bookings: from n/a through 1.15.78. **CVE ID : CVE-2023-32747**	N/A	A-AUT-WOOC-160124/47
Product: woocommerce_gocardless					
Affected Version(s): * Up to (excluding) 2.5.7					
Authorization Bypass Through User-Controlled Key	20-Dec-2023	7.5	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce WooCommerce GoCardless.This issue affects	N/A	A-AUT-WOOC-160124/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GoCardless: from n/a through 2.5.6. **CVE ID : CVE-2023-37871**		
Product: woocommerce_square					
Affected Version(s): * Up to (excluding) 3.8.2					
Authorization Bypass Through User-Controlled Key	20-Dec-2023	8.1	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce WooCommerce Square.This issue affects WooCommerce Square: from n/a through 3.8.1. **CVE ID : CVE-2023-35876**	N/A	A-AUT-WOOC-160124/49
Product: woocommerce_subscriptions					
Affected Version(s): * Up to (excluding) 5.1.3					
Authorization Bypass Through User-Controlled Key	20-Dec-2023	7.5	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce Woo Subscriptions.This issue affects Woo Subscriptions: from n/a through 5.1.2.	N/A	A-AUT-WOOC-160124/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35914		
Product: woopayments					
Affected Version(s): * Up to (excluding) 5.9.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Automattic WooPayments – Fully Integrated Solution Built and Supported by Woo.This issue affects WooPayments – Fully Integrated Solution Built and Supported by Woo: from n/a through 5.9.0. **CVE ID : CVE-2023-35915**	N/A	A-AUT-WOOP-160124/51
Authorization Bypass Through User-Controlled Key	20-Dec-2023	7.5	Authorization Bypass Through User-Controlled Key vulnerability in Automattic WooPayments – Fully Integrated Solution Built and Supported by Woo.This issue affects WooPayments – Fully Integrated Solution Built and	N/A	A-AUT-WOOP-160124/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Supported by Woo: from n/a through 5.9.0. **CVE ID : CVE-2023-35916**		
Vendor: averta					
Product: master_slider_pro					
Affected Version(s): * Up to (including) 3.6.5					
Deserialization of Untrusted Data	20-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in Master Slider Master Slider Pro.This issue affects Master Slider Pro: from n/a through 3.6.5. **CVE ID : CVE-2023-47507**	N/A	A-AVE-MAST-160124/53
Vendor: awplife					
Product: event_monster					
Affected Version(s): * Up to (including) 1.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in A WP Life Event Monster – Event Management, Tickets Booking, Upcoming Event allows Stored	N/A	A-AWP-EVEN-160124/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XSS.This issue affects Event Monster – Event Management, Tickets Booking, Upcoming Event: from n/a through 1.3.2. **CVE ID : CVE-2023-47525**		
Vendor: backupbliss					
Product: backup_migration					
Affected Version(s): * Up to (excluding) 1.4.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Dec-2023	9.8	The Backup Migration plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.3.9 via the 'content-backups' and 'content-name', 'content-manifest', or 'content-bmitmp' and 'content-identy' HTTP headers. This makes it possible for unauthenticated attackers to delete arbitrary files, including the wp-config.php file, which can make site takeover and remote code execution possible.	https://www.wordfence.com/threat-intel/vulnerabilities/id/0a3ae696-f67d-4ed2-b307-d2f36b6f188c?source=cve, https://plugins.trac.wordpress.org/browser/backup-backup/tags/1.3.9/includes/backup-heart.php	A-BAC-BACK-160124/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6972		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Dec-2023	7.2	The Backup Migration plugin for WordPress is vulnerable to OS Command Injection in all versions up to, and including, 1.3.9 via the 'url' parameter. This vulnerability allows authenticated attackers, with administrator-level permissions and above, to execute arbitrary commands on the host operating system. **CVE ID : CVE-2023-7002**	https://www.linuxquestions.org/questions/linux-security-4/php-function-exec-enabled-how-big-issue-4175508082/, https://plugins.trac.wordpress.org/changeset/3012745/backup-backup	A-BAC-BACK-160124/56
Affected Version(s): From (including) 1.0.8 Up to (excluding) 1.4.0					
Inclusion of Functionality from Untrusted Control Sphere	23-Dec-2023	9.8	The Backup Migration plugin for WordPress is vulnerable to Remote File Inclusion in versions 1.0.8 to 1.3.9 via the 'content-dir' HTTP header. This makes it possible for unauthenticated attackers to include remote files on the server, resulting in code execution. NOTE: Successful	https://www.wordfence.com/threat-intel/vulnerabilities/id/b380283c-0dbb-4d67-9f66-cb7c400c0427?source=cve, https://plugins.trac.wordpress.org/browser/backup-backup/tags/1.3.9/includes/backup-heart.php	A-BAC-BACK-160124/57

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability requires that the target server's php.ini is configured with 'allow_url_include' set to 'on'. This feature is deprecated as of PHP 7.4 and is disabled by default, but can still be explicitly enabled in later versions of PHP. **CVE ID : CVE-2023-6971**		
Vendor: Bannersky					
Product: bsk_forms_blacklist					
Affected Version(s): * Up to (excluding) 3.6.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	6.5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BannerSky BSK Forms Blacklist.This issue affects BSK Forms Blacklist: from n/a through 3.6.2. **CVE ID : CVE-2023-30872**	N/A	A-BAN-BSK_-160124/58
Vendor: bcoin					
Product: bcoin					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.2.0					
Use of a Broken or Risky Cryptographic Algorithm	21-Dec-2023	9.1	An issue was discovered in bcoin-org bcoin version 2.2.0, allows remote attackers to obtain sensitive information via weak hashing algorithms in the component \vendor\faye-websocket.js. **CVE ID : CVE-2023-50475**	N/A	A-BCO-BCOI-160124/59
Vendor: Bestwebsoft					
Product: contact_form_to_db					
Affected Version(s): * Up to (including) 1.7.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in BestWebSoft Contact Form to DB by BestWebSoft – Messages Database Plugin For WordPress.This issue affects Contact Form to DB by BestWebSoft – Messages Database Plugin For WordPress: from n/a through 1.7.0.	N/A	A-BES-CONT-160124/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29096		
Vendor: bigcommerce					
Product: bigcommerce					
Affected Version(s): * Up to (including) 5.0.6					
Exposure of Sensitive Information to an Unauthorized Actor	21-Dec-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in BigCommerce BigCommerce For WordPress.This issue affects BigCommerce For WordPress: from n/a through 5.0.6. **CVE ID : CVE-2023-49162**	N/A	A-BIG-BIGC-160124/61
Vendor: billahmed					
Product: qbit_matui					
Affected Version(s): 1.16.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Cross-Site Scripting (XSS) vulnerability in bill-ahmed qbit-matUI version 1.16.4, allows remote attackers to obtain sensitive information via fixed session identifiers (SID) in index.js file. **CVE ID : CVE-2023-50473**	N/A	A-BIL-QBIT-160124/62
Vendor: binarycarpenter					
Product: menu_bar_cart_icon_for_woocommerce					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.49.3					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in BinaryCarpenter Menu Bar Cart Icon For WooCommerce By Binary Carpenter.This issue affects Menu Bar Cart Icon For WooCommerce By Binary Carpenter: from n/a through 1.49.3. **CVE ID : CVE-2023-49855**	N/A	A-BIN-MENU-160124/63
Vendor: Bitvise					
Product: ssh_client					
Affected Version(s): * Up to (excluding) 9.33					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-BIT-SSH_-160124/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypt		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			o before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: ssh_server					
Affected Version(s): * Up to (excluding) 9.32					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-BIT-SSH_-160124/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: blazzdev					
Product: rate_my_post					
Affected Version(s): * Up to (excluding) 3.4.2					
Authorization Bypass Through User-Controlled Key	21-Dec-2023	6.5	Authorization Bypass Through User-Controlled Key vulnerability in Blaz K. Rate my Post – WP Rating System.This issue affects Rate my Post – WP Rating System: from n/a through 3.4.1. **CVE ID : CVE-2023-49765**	N/A	A-BLA-RATE-160124/66
Vendor: blinksocks					
Product: blinksocks					
Affected Version(s): 3.3.8					
Use of a Broken or Risky	21-Dec-2023	7.5	An issue was discovered in blinksocks version	N/A	A-BLI-BLIN-160124/67

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			3.3.8, allows remote attackers to obtain sensitive information via weak encryption algorithms in the component /presets/ssr-auth-chain.js. **CVE ID : CVE-2023-50481**		
Vendor: bluecoral					
Product: chat_bubble					
Affected Version(s): * Up to (including) 2.3					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Blue Coral Chat Bubble – Floating Chat with Contact Chat Icons, Messages, Telegram, Email, SMS, Call me back.This issue affects Chat Bubble – Floating Chat with Contact Chat Icons, Messages, Telegram, Email, SMS, Call me back: from n/a through 2.3. **CVE ID : CVE-2023-48769**	N/A	A-BLU-CHAT-160124/68
Vendor: bosch					
Product: bosch_video_management_system					
Affected Version(s): * Up to (including) 12.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-BOSC-160124/69
Product: building_integration_system_video_engine					
Affected Version(s): * Up to (including) 5.0.1					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-BUIL-160124/70

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: configuration_manager					
Affected Version(s): * Up to (including) 7.62					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-CONF-160124/71
Product: intelligent_insights					
Affected Version(s): * Up to (including) 1.0.3.14					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks.	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-INTE-160124/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35867		
Product: monitor_wall					
Affected Version(s): * Up to (including) 10.00.0164					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-MONI-160124/73
Product: project_assistant					
Affected Version(s): * Up to (including) 2.3					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-PROJ-160124/74
Product: video_management_system_viewer					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 12.0					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-VIDE-160124/75
Product: video_recording_manager					
Affected Version(s): * Up to (including) 04.10.0079					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-VIDE-160124/76
Product: video_security_client					
Affected Version(s): * Up to (including) 3.3.5					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API	https://psirt.bosch.com/security-y-	A-BOS-VIDE-160124/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	advisories/BOSCH-SA-092656-BT.html	
Product: video_streaming_gateway					
Affected Version(s): * Up to (including) 8.1.2.2					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-VIDE-160124/78
Affected Version(s): From (including) 9.0.0 Up to (including) 9.0.0.178					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-VIDE-160124/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**		
Product: _onvif_camera_event_driver_tool					
Affected Version(s): * Up to (including) 2.0.0.8					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	A-BOS-_ONV-160124/80
Vendor: c-blosc2_project					
Product: c-blosc2					
Affected Version(s): * Up to (excluding) 2.9.3					
NULL Pointer Dereference	25-Dec-2023	7.5	C-blosc2 before 2.9.3 was discovered to contain a NULL pointer dereference via the function zfp_prec_decompress at zfp/blosc2-zfp.c.	https://github.com/Blosc/c-blosc2/issues/519, https://github.com/Blosc/c-blosc2/commit/425e8a9a59d49378d57e2116b6c9b0190a5986f5	A-C-B-C-BL-160124/81

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37185		
NULL Pointer Dereference	25-Dec-2023	7.5	C-blosc2 before 2.9.3 was discovered to contain a NULL pointer dereference in ndlz/ndlz8x8.c via a NULL pointer to memset. **CVE ID : CVE-2023-37186**	https://github.com/Blosc/c-blosc2/issues/522, https://github.com/Blosc/c-blosc2/commit/d55bfcd6804699e1435dc3e233fd76c8a5d3f9e3	A-C-B-C-BL-160124/82
NULL Pointer Dereference	25-Dec-2023	7.5	C-blosc2 before 2.9.3 was discovered to contain a NULL pointer dereference via the zfp/blosc2-zfp.c zfp_acc_decompress. function. **CVE ID : CVE-2023-37187**	https://github.com/Blosc/c-blosc2/commit/425e8a9a59d49378d57e2116b6c9b0190a5986f5, https://github.com/Blosc/c-blosc2/issues/520	A-C-B-C-BL-160124/83
NULL Pointer Dereference	25-Dec-2023	7.5	C-blosc2 before 2.9.3 was discovered to contain a NULL pointer dereference via the function zfp_rate_decompress at zfp/blosc2-zfp.c. **CVE ID : CVE-2023-37188**	https://github.com/Blosc/c-blosc2/commit/425e8a9a59d49378d57e2116b6c9b0190a5986f5, https://github.com/Blosc/c-blosc2/issues/521	A-C-B-C-BL-160124/84
Vendor: Cacti					
Product: cacti					
Affected Version(s): * Up to (excluding) 1.2.25					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	4.8	Cacti is an open source operational monitoring and fault management framework. The fix applied for CVE-2023-39515 in version 1.2.25 is incomplete as it enables an adversary to have a victim browser execute malicious code when a victim user hovers their mouse over the malicious data source path in `data_debug.php`. To perform the cross-site scripting attack, the adversary needs to be an authorized cacti user with the following permissions: `General Administration>Sites/Devices/Data`. The victim of this attack could be any account with permissions to view `http://<HOST>/cacti/data_debug.php`. As of time of publication, no complete fix has been included in Cacti.	https://github.com/Cacti/cacti/security/advisories/GHSA-q7g7-gcf6-wh4x, https://github.com/Cacti/cacti/security/advisories/GHSA-hrg9-qqqx-wc4h, https://github.com/Cacti/cacti/blob/5f6f65c215d663a775950b2d9db35edbaf07d680/data_debug.php	A-CAC-CACT-160124/85

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49088		
Affected Version(s): * Up to (including) 1.2.25					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	8.8	Cacti provides an operational monitoring and fault management framework. In versions 1.2.25 and prior, it is possible to execute arbitrary SQL code through the `pollers.php` script. An authorized user may be able to execute arbitrary SQL code. The vulnerable component is the `pollers.php`. Impact of the vulnerability - arbitrary SQL code execution. As of time of publication, a patch does not appear to exist. **CVE ID : CVE-2023-49085**	https://github.com/Cacti/cacti/security/advisories/GHSA-vr3c-38wh-g855, https://github.com/Cacti/cacti/blob/5f6f65c215d663a775950b2d9db35edbaf07d680/pollers.php#L451	A-CAC-CACT-160124/86
Affected Version(s): 1.2.25					
Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote	21-Dec-2023	8.8	Cacti is a robust performance and fault management framework and a frontend to RRDTool - a Time Series Database (TSDB). While using the detected SQL Injection and insufficient	https://github.com/Cacti/cacti/security/advisories/GHSA-pfh9-gwm6-86vp	A-CAC-CACT-160124/87

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File Inclusion')			processing of the include file path, it is possible to execute arbitrary code on the server. Exploitation of the vulnerability is possible for an authorized user. The vulnerable component is the `link.php`. Impact of the vulnerability execution of arbitrary code on the server. **CVE ID : CVE-2023-49084**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	8.8	Cacti provides an operational monitoring and fault management framework. Version 1.2.25 has a Blind SQL Injection (SQLi) vulnerability within the SNMP Notification Receivers feature in the file `‘managers.php’`. An authenticated attacker with the “Settings/Utilities” permission can send a crafted HTTP GET request to the endpoint `‘/cacti/managers.php’` with an SQLi payload in the `‘selected_graphs_a	https://github.com/Cacti/cacti/security/advisories/GHSA-w85f-7c4w-7594, https://github.com/Cacti/cacti/blob/5f6f65c215d663a775950b2d9db35edbaf07d680/managers.php#L941	A-CAC-CACT-160124/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rray`` HTTP GET parameter. As of time of publication, no patched versions exist. **CVE ID : CVE-2023-51448**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	6.1	Cacti is an open source operational monitoring and fault management framework. A reflection cross-site scripting vulnerability was discovered in version 1.2.25. Attackers can exploit this vulnerability to perform actions on behalf of other users. The vulnerability is found in `templates_import.php.` When uploading an xml template file, if the XML file does not pass the check, the server will give a JavaScript pop-up prompt, which contains unfiltered xml template file name, resulting in XSS. An attacker exploiting this vulnerability could execute actions on behalf of other users. This ability	https://github.com/Cacti/cacti/security/advisories/GHSA-xwqc-7jc4-xm73, https://github.com/Cacti/cacti/blob/5f6f65c215d663a775950b2d9db35edbaf07d680/templates_import.php	A-CAC-CACT-160124/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to impersonate users could lead to unauthorized changes to settings. As of time of publication, no patched versions are available. **CVE ID : CVE-2023-50250**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	6.1	Reflected Cross Site Scripting (XSS) vulnerability in Cacti v1.2.25, allows remote attackers to escalate privileges when uploading an xml template file via templates_import.php. **CVE ID : CVE-2023-50569**	https://github.com/Cacti/cacti/security/advisories/GHSA-xwqc-7jc4-xm73	A-CAC-CACT-160124/90
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	5.4	Cacti is a robust performance and fault management framework and a frontend to RRDTool - a Time Series Database (TSDB). Bypassing an earlier fix (CVE-2023-39360) that leads to a DOM XSS attack. Exploitation of the vulnerability is possible for an authorized user.	https://github.com/Cacti/cacti/security/advisories/GHSA-wc73-r2vw-59pr	A-CAC-CACT-160124/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The vulnerable component is the `graphs_new.php`. Impact of the vulnerability - execution of arbitrary javascript code in the attacked user's browser. This issue has been patched in version 1.2.26. **CVE ID : CVE-2023-49086**		
Vendor: carmelogarcia					
Product: faculty_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Dec-2023	9.8	A vulnerability was found in code-projects Faculty Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/php/crud.php. The manipulation of the argument fieldname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may	N/A	A-CAR-FACU-160124/92

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used. The identifier of this vulnerability is VDB-248948. **CVE ID : CVE-2023-7096**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	6.1	A vulnerability, which was classified as problematic, has been found in code-projects Faculty Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/pages/yearlevel.php. The manipulation of the argument Year Level/Section leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248744. **CVE ID : CVE-2023-7057**	N/A	A-CAR-FACU-160124/93
Improper Neutralization of Input During	22-Dec-2023	5.4	A vulnerability classified as problematic was found in code-projects Faculty	N/A	A-CAR-FACU-160124/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/pages/subjects.php. The manipulation of the argument Description/Units 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-248743. **CVE ID : CVE-2023-7056**		
Vendor: Cesanta					
Product: mjs					
Affected Version(s): 2.22.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2023	9.8	Cesanta MJS 2.20.0 has a getprop_builtin_foreign out-of-bounds read if a Built-in API name occurs in a substring of an input string. **CVE ID : CVE-2023-50044**	https://github.com/cesanta/mjs/pull/255	A-CES-MJS-160124/95
Vendor: Clear					
Product: clearml_server					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.13.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository allegroai/clearml-server prior to 1.13.0. This vulnerability affects the ClearML Open Source Server which is not designed to be used as a publicly available service. Security recommendations stress it should be placed behind a company firewall or VPN. This vulnerability only affects users within the same organisation (I.e when a malicious party already has access to the internal network and to a user's ClearML login credentials). **CVE ID : CVE-2023-6778**	https://huntr.com/bounties/5f3fffac-0358-48e6-a500-81bac13e0e2b, https://github.com/allegroai/clearml-server/commit/4684fd5b74af582c894b67a0a06e865c948b763a	A-CLE-CLEA-160124/96
Vendor: cleverplugins					
Product: delete_duplicate_posts					
Affected Version(s): * Up to (including) 4.8.9					
Missing Authorization	19-Dec-2023	9.8	Missing Authorization vulnerability in Clever plugins Delete Duplicate Posts allows	N/A	A-CLE-DELE-160124/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Accessing Functionality Not Properly Constrained by ACLs.This issue affects Delete Duplicate Posts: from n/a through 4.8.9. **CVE ID : CVE-2023-47754**		
Vendor: Cminds					
Product: cm_popup					
Affected Version(s): * Up to (excluding) 1.6.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	8.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CreativeMindsSolutions CM Popup Plugin for WordPress.This issue affects CM Popup Plugin for WordPress: from n/a through 1.5.10. **CVE ID : CVE-2023-30750**	N/A	A-CMI-CM_P-160124/98
Vendor: code-projects					
Product: point_of_sales_and_inventory_management_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	6.1	A vulnerability was found in code-projects Point of Sales and Inventory Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /main/checkout.php. The manipulation of the argument pt leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-248846 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-7075**	N/A	A-COD-POIN-160124/99
Vendor: codeastrology					
Product: add_to_cart_text_changer_and_customize_button\,_add_custom_icon					
Affected Version(s): * Up to (including) 2.0					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Saiful Islam Add to Cart Text Changer and Customize Button, Add	N/A	A-COD-ADD_-160124/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Custom Icon.This issue affects Add to Cart Text Changer and Customize Button, Add Custom Icon: from n/a through 2.0. **CVE ID : CVE-2023-49153**		
Product: quantity_plus_minus_button_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.2.0					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in CodeAstrology Team Quantity Plus Minus Button for WooCommerce by CodeAstrology.This issue affects Quantity Plus Minus Button for WooCommerce by CodeAstrology: from n/a through 1.1.9. **CVE ID : CVE-2023-48768**	N/A	A-COD-QUAN-160124/101
Vendor: codelyfe					
Product: stupid_simple_cms					
Affected Version(s): * Up to (including) 1.2.4					
Unrestricted Upload of File with	17-Dec-2023	9.8	A vulnerability has been found in codelyfe Stupid Simple CMS up to 1.2.4 and classified	N/A	A-COD-STUP-160124/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			as critical. This vulnerability affects unknown code of the file /file-manager/upload.php. The manipulation of the argument file leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248260. **CVE ID : CVE-2023-6902**		
Improper Authentication	18-Dec-2023	9.1	A vulnerability has been found in codelyfe Stupid Simple CMS up to 1.2.4 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /file-manager/delete.php of the component Deletion Interface. The manipulation of the argument file leads to improper authentication. The exploit has been disclosed to the public and may be used. The identifier VDB-248269 was	N/A	A-COD-STUP-160124/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-6907**		
Path Traversal: '../filedir'	21-Dec-2023	6.5	A vulnerability classified as problematic was found in codelyfe Stupid Simple CMS up to 1.2.4. Affected by this vulnerability is an unknown functionality of the file /file-manager/rename.php. The manipulation of the argument oldName leads to path traversal: '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248689 was assigned to this vulnerability. **CVE ID : CVE-2023-7040**	N/A	A-COD-STUP-160124/104
Path Traversal: '../filedir'	21-Dec-2023	5.4	A vulnerability, which was classified as critical, has been found in codelyfe Stupid Simple CMS up to 1.2.4. Affected by this issue is some	N/A	A-COD-STUP-160124/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unknown functionality of the file /file-manager/rename.php. The manipulation of the argument newName leads to path traversal: '../filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-248690 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-7041**		
Affected Version(s): From (including) 1.1.7 Up to (including) 1.2.3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Dec-2023	9.8	A vulnerability, which was classified as critical, was found in codelyfe Stupid Simple CMS up to 1.2.3. This affects an unknown part of the file /terminal/handle-command.php of the component HTTP POST Request Handler. The manipulation of the argument command with the input whoami leads to os command	N/A	A-COD-STUP-160124/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			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-248259. **CVE ID : CVE-2023-6901**		
Vendor: codesmade					
Product: autocomplete_location_field_contact_form_7					
Affected Version(s): * Up to (excluding) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	The Autocomplete Location field Contact Form 7 WordPress plugin before 3.0, autocomplete-location-field-contact-form-7-pro WordPress plugin before 2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	N/A	A-COD-AUTO-160124/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5005		
Affected Version(s): * Up to (excluding) 3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	The Autocomplete Location field Contact Form 7 WordPress plugin before 3.0, autocomplete-location-field-contact-form-7-pro WordPress plugin before 2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup) **CVE ID : CVE-2023-5005**	N/A	A-COD-AUTO-160124/108
Vendor: concretecms					
Product: concrete_cms					
Affected Version(s): From (including) 9.0 Up to (excluding) 9.2.3					
Cross-Site Request Forgery (CSRF)	25-Dec-2023	4.3	Concrete CMS 9 before 9.2.3 is vulnerable to Cross Site Request Forgery (CSRF) via /ccm/system/dialogs/logs/delete_all/submit. An attacker can force an admin user to delete	https://www.concretecms.org/about/project-news/security/2023-12-05-concrete-cms-new-cves-and-cve-updates	A-CON-CONC-160124/109

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server report logs on a web application to which they are currently authenticated. **CVE ID : CVE-2023-48652**		
Vendor: connectbot					
Product: sshlib					
Affected Version(s): * Up to (excluding) 2.2.22					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions,	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-CON-SSHL-160124/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js,		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: crates					
Product: thrussh					
Affected Version(s): * Up to (excluding) 0.35.1					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-CRA-THRU-160124/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: crawlspider					
Product: seo_change_monitor					
Affected Version(s): * Up to (excluding) 1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	8.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CrawlSpider SEO Change Monitor – Track Website Changes.This issue affects SEO Change Monitor – Track Website Changes: from n/a through 1.2. **CVE ID : CVE-2023-33209**	N/A	A-CRA-SEO_-160124/112
Vendor: creatomatic					
Product: csprite					
Affected Version(s): * Up to (including) 1.1					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Creatomatic Ltd CSprite.This issue affects CSprite: from n/a through 1.1.	N/A	A-CRE-CSPR-160124/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49763		
Vendor: crmperks					
Product: integration_for_salesforce_and_contact_form_7\,_wpforms\,_elementor\,_ninja_forms					
Affected Version(s): * Up to (including) 1.3.3					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2023	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Integration for Salesforce and Contact Form 7, WPForms, Elementor, Ninja Forms.This issue affects Integration for Salesforce and Contact Form 7, WPForms, Elementor, Ninja Forms: from n/a through 1.3.3. **CVE ID : CVE-2023-37982**	N/A	A-CRM-INTE-160124/114
Product: integration_for_woocommerce_and_quickbooks					
Affected Version(s): * Up to (including) 1.2.3					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2023	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Integration for WooCommerce and QuickBooks.This	N/A	A-CRM-INTE-160124/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Integration for WooCommerce and QuickBooks: from n/a through 1.2.3. **CVE ID : CVE-2023-38478**		
Product: integration_for_woocommerce_and_zoho_crm\,_books\,_invoice\,_inventory\,_bigin					
Affected Version(s): * Up to (excluding) 1.3.7					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2023	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Integration for WooCommerce and Zoho CRM, Books, Invoice, Inventory, Bigin.This issue affects Integration for WooCommerce and Zoho CRM, Books, Invoice, Inventory, Bigin: from n/a before 1.3.7. **CVE ID : CVE-2023-38481**	N/A	A-CRM-INTE-160124/116
Vendor: crocoblock					
Product: jetelements_for_elementor					
Affected Version(s): * Up to (excluding) 2.6.13.1					
Cross-Site Request	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Crocoblock	N/A	A-CRO-JETE-160124/117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			JetElements For Elementor.This issue affects JetElements For Elementor: from n/a through 2.6.13. **CVE ID : CVE-2023-48762**		
Vendor: crushftp					
Product: crushftp					
Affected Version(s): * Up to (excluding) 10.6.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP),	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-CRU-CRUS-160124/118

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Affected Version(s): * Up to (including) 10.6.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-CRU-CRUS-160124/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Cryptopp					
Product: crypto\+\+					
Affected Version(s): * Up to (including) 8.9.0					
N/A	18-Dec-2023	7.5	gf2n.cpp in Crypto++ (aka cryptopp) through 8.9.0 allows attackers to cause a denial of service (application crash) via DER public-key data for an F(2^m) curve, if the degree of each term in the polynomial is not strictly decreasing. **CVE ID : CVE-2023-50980**	N/A	A-CRY-CRYP-160124/120
Loop with Unreachable Exit Condition ('Infinite Loop')	18-Dec-2023	7.5	ModularSquareRoot in Crypto++ (aka cryptopp) through 8.9.0 allows attackers to cause a denial of service (infinite loop) via crafted DER public-key data associated with squared odd numbers, such as the square of 268995137513890432434389773128616504853. **CVE ID : CVE-2023-50981**	N/A	A-CRY-CRYP-160124/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	18-Dec-2023	5.9	Crypto++ (aka cryptopp) through 8.9.0 has a Marvin side channel during decryption with PKCS#1 v1.5 padding. **CVE ID : CVE-2023-50979**	N/A	A-CRY-CRYP-160124/122
Vendor: cuppacms					
Product: cuppacms					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	SQL Injection vulnerability in components/table_manager/html/edit_admin_table.php in CuppaCMS V1.0 allows attackers to run arbitrary SQL commands via the table parameter. **CVE ID : CVE-2023-47990**	N/A	A-CUP-CUPP-160124/123
Vendor: davidvongries					
Product: ultimate_dashboard					
Affected Version(s): * Up to (including) 3.7.11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Vongries Ultimate Dashboard – Custom WordPress Dashboard allows Stored XSS.This issue affects	N/A	A-DAV-ULTI-160124/124

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ultimate Dashboard – Custom WordPress Dashboard: from n/a through 3.7.11. **CVE ID : CVE-2023-50828**		
Vendor: Dell					
Product: emc_networker					
Affected Version(s): * Up to (including) 19.8					
Use of a Broken or Risky Cryptographic Algorithm	18-Dec-2023	5.3	Dell NetWorker Virtual Edition versions 19.8 and below contain the use of deprecated cryptographic algorithms in the SSH component. A remote unauthenticated attacker could potentially exploit this vulnerability leading to some information disclosure. **CVE ID : CVE-2023-28053**	https://www.dell.com/support/kbdoc/en-us/000220547/dsa-2023-358-security-update-for-dell-networker-virtual-edition-ssh-cryptographic-vulnerabilities	A-DEL-EMC_-160124/125
Vendor: dfirkuiper					
Product: kuiper					
Affected Version(s): 2.3.4					
Improper Limitation of a	18-Dec-2023	5.9	A vulnerability, which was classified as	https://github.com/DFIRKuiper/Kuiper/pull/1	A-DFI-KUIP-160124/126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			problematic, was found in DFIRKuiper Kuiper 2.3.4. This affects the function unzip_file of the file kuiper/app/controllers/case_management.py of the component TAR Archive Handler. The manipulation of the argument dst_path leads to path traversal. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 2.3.5 is able to address this issue. The identifier of the patch is 94fa135153002f651f5526c55a7240e083db8d73. It is recommended to upgrade the affected component. The identifier VDB-248277 was assigned to this vulnerability. **CVE ID : CVE-2023-6908**	06, https://github.com/DFIRKuiper/Kuiper/commit/94fa135153002f651f5526c55a7240e083db8d73	
Vendor: dmry					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sayfa_sayac					
Affected Version(s): * Up to (including) 2.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Hakan Demiray Sayfa Sayac.This issue affects Sayfa Sayac: from n/a through 2.6. **CVE ID : CVE-2023-49776**	N/A	A-DMR-SAYF-160124/127
Deserialization of Untrusted Data	21-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in Hakan Demiray Sayfa Sayac.This issue affects Sayfa Sayac: from n/a through 2.6. **CVE ID : CVE-2023-49778**	N/A	A-DMR-SAYF-160124/128
Vendor: doofinder					
Product: doofinder					
Affected Version(s): * Up to (including) 1.5.49					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2023	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Doofinder Doofinder WP & WooCommerce	N/A	A-DOO-DOOF-160124/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Search.This issue affects Doofinder WP & WooCommerce Search: from n/a through 1.5.49. **CVE ID : CVE-2023-40602**		
Vendor: dropbear_ssh_project					
Product: dropbear_ssh					
Affected Version(s): * Up to (excluding) 2022.83					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP),	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-DRO-DROP-160124/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: e2pdf					
Product: e2pdf					
Affected Version(s): * Up to (including) 1.20.18					
Deserialization of Untrusted Data	19-Dec-2023	7.2	Deserialization of Untrusted Data vulnerability in E2Pdf.Com E2Pdf – Export To Pdf Tool for WordPress.This issue affects E2Pdf – Export To Pdf Tool for WordPress: from n/a through 1.20.18. **CVE ID : CVE-2023-46154**	N/A	A-E2P-E2PD-160124/131
Vendor: elearningfreak					
Product: insert_or_embed_articulate_content					
Affected Version(s): * Up to (including) 4.3000000021					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brian Batt Insert or Embed Articulate	N/A	A-ELE-INSE-160124/132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Content into WordPress allows Stored XSS.This issue affects Insert or Embed Articulate Content into WordPress: from n/a through 4.3000000021. **CVE ID : CVE-2023-50824**		
Vendor: elegantthemes					
Product: divi					
Affected Version(s): * Up to (excluding) 4.23.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-2023	5.4	The Divi theme for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'et_pb_text' shortcode in all versions up to, and including, 4.23.1 due to insufficient input sanitization and output escaping on user supplied custom field data. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever	N/A	A-ELE-DIVI-160124/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a user accesses an injected page. **CVE ID : CVE-2023-6744**		
Vendor: Erlang					
Product: erlang\/otp					
Affected Version(s): * Up to (excluding) 26.2.1					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-ERL-ERLA-160124/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: esiteq					
Product: wp_report_post					
Affected Version(s): * Up to (including) 2.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Dec-2023	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Alex Raven WP Report Post allows SQL Injection.This issue affects WP Report Post: from n/a through 2.1.2. **CVE ID : CVE-2023-34168**	N/A	A-ESI-WP_R-160124/135
Vendor: extendthemes					
Product: colibri_page_builder					
Affected Version(s): * Up to (including) 1.0.239					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ExtendThemes Colibri Page Builder allows Stored XSS.This issue affects Colibri Page Builder: from	N/A	A-EXT-COLI-160124/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			n/a through 1.0.239. **CVE ID : CVE-2023-50833**		
Vendor: fabianros					
Product: library_management_system					
Affected Version(s): 2.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Dec-2023	9.8	A vulnerability, which was classified as critical, was found in code-projects Library Management System 2.0. Affected is an unknown function of the file index.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. VDB-249006 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-7111**	N/A	A-FAB-LIBR-160124/137
Product: water_billing_system					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Dec-2023	9.8	A vulnerability classified as critical has been found in code-projects Water Billing System 1.0. This affects an unknown part of the file /addbill.php. The manipulation of the argument owners_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248949 was assigned to this vulnerability. **CVE ID : CVE-2023-7097**	N/A	A-FAB-WATE-160124/138
Vendor: favethemes					
Product: houzez					
Affected Version(s): * Up to (excluding) 2.8.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Favethemes Houzez - Real Estate WordPress Theme.This issue affects Houzez - Real Estate WordPress Theme:	N/A	A-FAV-HOUZ-160124/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			from n/a before 2.8.3. **CVE ID : CVE-2023-29432**		
Vendor: filezilla-project					
Product: filezilla_client					
Affected Version(s): * Up to (excluding) 3.66.4					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-FIL-FILE-160124/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: forestblog_project					
Product: forestblog					
Affected Version(s): * Up to (including) 2022-06-30					
Unrestricted Upload of File with Dangerous Type	17-Dec-2023	9.8	A vulnerability classified as critical has been found in saysky ForestBlog up to 20220630. This affects an unknown part of the file /admin/upload/img of the component Image Upload Handler. The manipulation of the argument filename leads to unrestricted upload. 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-248247. **CVE ID : CVE-2023-6887**	N/A	A-FOR-FORE-160124/141
Vendor: foxskav					
Product: easy_bet					
Affected Version(s): * Up to (including) 1.0.2					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	8.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Foxskav Easy Bet.This issue affects Easy Bet: from n/a through 1.0.2. **CVE ID : CVE-2023-31092**	N/A	A-FOX-EASY-160124/142
Vendor: freshlightlab					
Product: menu_image\,_icons_made_easy					
Affected Version(s): * Up to (including) 3.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Freshlight Lab Menu Image, Icons made easy allows Stored XSS.This issue affects Menu Image, Icons made easy: from n/a through 3.10. **CVE ID : CVE-2023-50826**	N/A	A-FRE-MENU-160124/143
Vendor: gallagher					
Product: command_centre					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 8.50					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior.	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	A-GAL-COMM-160124/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22439		
Affected Version(s): 9.00.1507					
N/A	18-Dec-2023	7.1	A reliance on untrusted inputs in a security decision could be exploited by a privileged user to configure the Gallagher Command Centre Diagnostics Service to use less secure communication protocols. This issue affects: Gallagher Diagnostics Service prior to v1.3.0 (distributed in 9.00.1507(MR1)). **CVE ID : CVE-2023-46686**	https://security.gallagher.com/Security-Advisories/CVE-2023-46686	A-GAL-COMM-160124/145
Affected Version(s): From (including) 8.60 Up to (excluding) 8.60.231116a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	A-GAL-COMM-160124/146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Affected Version(s): From (including) 8.70 Up to (excluding) 8.70.231204a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	A-GAL-COMM-160124/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7000 optional diag nostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Affected Version(s): From (including) 8.80 Up to (excluding) 8.80.231204a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	A-GAL-COMM-160124/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6000 and Controller 7000 optional diagnostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Affected Version(s): From (including) 8.90 Up to (excluding) 8.90.231204a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a	https://security.gallagher.com/Security-	A-GAL-COMM-160124/149

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**	Advisories/CVE-2023-22439	
Affected Version(s): From (including) 9.00 Up to (excluding) 9.00.1507					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Dec-2023	7.1	A reliance on untrusted inputs in a security decision could be exploited by a privileged user to configure the Gallagher Command Centre Diagnostics Service to use less secure communication protocols. This issue affects: Gallagher Diagnostics Service prior to v1.3.0 (distributed in 9.00.1507(MR1)). **CVE ID : CVE-2023-46686**	https://security.gallagher.com/Security-Advisories/CVE-2023-46686	A-GAL-COMM-160124/150
Vendor: gamipress					
Product: gamipress					
Affected Version(s): * Up to (including) 2.5.6					
Missing Authorization	19-Dec-2023	6.5	Missing Authorization vulnerability in GamiPress GamiPress – The #1 gamification plugin to reward points, achievements, badges & ranks in	N/A	A-GAM-GAMI-160124/151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress.This issue affects GamiPress – The #1 gamification plugin to reward points, achievements, badges & ranks in WordPress: from n/a through 2.5.6. **CVE ID : CVE-2023-25715**		
Vendor: Gentoo					
Product: security					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack.	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-GEN-SECU-160124/152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: getbutterfly					
Product: block_for_font_awesome					
Affected Version(s): * Up to (including) 1.4.0					
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ciprian Popescu Block for Font Awesome.This issue affects Block for Font Awesome: from n/a through 1.4.0. **CVE ID : CVE-2023-49751**	N/A	A-GET-BLOC-160124/153
Vendor: getshortcodes					
Product: shortcodes_ultimate					
Affected Version(s): * Up to (including) 7.0.0					
Improper Neutralization of Input During Web Page Generation	19-Dec-2023	5.4	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site	https://plugins.trac.wordpress.org/browser/shortcodes-ultimate/trunk/includes/shortc	A-GET-SHOR-160124/154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting via the plugin's 'su_button', 'su_members', and 'su_tabs' shortcodes in all versions up to, and including, 7.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-6488**	odes/button.php	
Vendor: giannopouloskostas					
Product: wpsoononlinepage					
Affected Version(s): * Up to (including) 1.9					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Giannopoulos Kostas WPsoonOnlinePage .This issue affects WPsoonOnlinePage : from n/a through 1.9.	N/A	A-GIA-WPSO-160124/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49760		
Vendor: Github					
Product: enterprise_server					
Affected Version(s): 3.11.0					
Insufficient Entropy	21-Dec-2023	7.5	An insufficient entropy vulnerability was identified in GitHub Enterprise Server (GHES) that allowed an attacker to brute force a user invitation to the GHES Management Console. To exploit this vulnerability, an attacker would need knowledge that a user invitation was pending. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-46648**	N/A	A-GIT-ENTE-160124/156

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	21-Dec-2023	7.5	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed a bypass of Private Mode by using a specially crafted API request. To exploit this vulnerability, an attacker would need network access to the Enterprise Server appliance configured in Private Mode. This vulnerability affected all versions of GitHub Enterprise Server since 3.9 and was fixed in version 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-6847**	N/A	A-GIT-ENTE-160124/157
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	7	A race condition in GitHub Enterprise Server was identified that could allow an attacker administrator access. To exploit this, an	N/A	A-GIT-ENTE-160124/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			organization needs to be converted from a user. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-46649**		
Insertion of Sensitive Information into Log File	21-Dec-2023	6.5	An insertion of sensitive information into the log file in the audit log in GitHub Enterprise Server was identified that could allow an attacker to gain access to the management console. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup archive created with GitHub Enterprise Server Backup Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was	N/A	A-GIT-ENTE-160124/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6802**		
Insertion of Sensitive Information into Log File	21-Dec-2023	5.7	An insertion of sensitive information into log file vulnerability was identified in the log files for a GitHub Enterprise Server back-end service that could permit an `adversary in the middle attack` when combined with other phishing techniques. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup archive created with GitHub Enterprise Server Backup Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12,	N/A	A-GIT-ENTE-160124/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6746**		
Improper Privilege Management	21-Dec-2023	5.5	Improper privilege management allowed arbitrary workflows to be committed and run using an improperly scoped PAT. To exploit this, a workflow must have already existed in the target repo. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6804**	N/A	A-GIT-ENTE-160124/161
Incorrect Authorization	21-Dec-2023	4.9	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be updated with an improperly scoped token. This vulnerability did not allow unauthorized access to any repository content	N/A	A-GIT-ENTE-160124/162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as it also required contents:write and issues:read permissions. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51379**		
Incorrect Authorization	21-Dec-2023	4.3	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be read with an improperly scoped token. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51380**	N/A	A-GIT-ENTE-160124/163
Time-of-check Time-of-use (TOCTOU)	21-Dec-2023	4	A race condition in GitHub Enterprise Server allows an outside collaborator to be added while a repository is being	N/A	A-GIT-ENTE-160124/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			transferred. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6803**		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	2	A race condition in GitHub Enterprise Server allowed an existing admin to maintain permissions on transferred repositories by making a GraphQL mutation to alter repository permissions during the transfer. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6690**	N/A	A-GIT-ENTE-160124/165
Affected Version(s): From (including) 3.10.0 Up to (excluding) 3.10.3					
Improper Privilege Management	21-Dec-2023	8.8	Improper privilege management in all versions of GitHub Enterprise Server allows users with	N/A	A-GIT-ENTE-160124/166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorized access to the management console with an editor role to escalate their privileges by making requests to the endpoint used for bootstrapping the instance. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.12, 3.9.6, 3.10.3, and 3.11.0. **CVE ID : CVE-2023-46647**		
Affected Version(s): From (including) 3.10.0 Up to (excluding) 3.10.4					
Insufficient Entropy	21-Dec-2023	7.5	An insufficient entropy vulnerability was identified in GitHub Enterprise Server (GHES) that allowed an attacker to brute force a user invitation to the GHES Management Console. To exploit this vulnerability, an attacker would need knowledge that a user invitation was pending. This vulnerability affected all versions of GitHub Enterprise Server	N/A	A-GIT-ENTE-160124/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-46648**		
Improper Authentication	21-Dec-2023	7.5	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed a bypass of Private Mode by using a specially crafted API request. To exploit this vulnerability, an attacker would need network access to the Enterprise Server appliance configured in Private Mode. This vulnerability affected all versions of GitHub Enterprise Server since 3.9 and was fixed in version 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	A-GIT-ENTE-160124/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6847		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	7	A race condition in GitHub Enterprise Server was identified that could allow an attacker administrator access. To exploit this, an organization needs to be converted from a user. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-46649**	N/A	A-GIT-ENTE-160124/169
Insertion of Sensitive Information into Log File	21-Dec-2023	6.5	An insertion of sensitive information into the log file in the audit log in GitHub Enterprise Server was identified that could allow an attacker to gain access to the management console. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup	N/A	A-GIT-ENTE-160124/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			archive created with GitHub Enterprise Server Backup Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6802**		
Insertion of Sensitive Information into Log File	21-Dec-2023	5.7	An insertion of sensitive information into log file vulnerability was identified in the log files for a GitHub Enterprise Server back-end service that could permit an `adversary in the middle attack` when combined with other phishing techniques. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup archive created with GitHub Enterprise Server Backup	N/A	A-GIT-ENTE-160124/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6746**		
Improper Privilege Management	21-Dec-2023	5.5	Improper privilege management allowed arbitrary workflows to be committed and run using an improperly scoped PAT. To exploit this, a workflow must have already existed in the target repo. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6804**	N/A	A-GIT-ENTE-160124/172
Authorization Bypass Through User-	21-Dec-2023	5.3	Improper access control in all versions of GitHub Enterprise Server	N/A	A-GIT-ENTE-160124/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			allows unauthorized users to view private repository names via the "Get a check run" API endpoint. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected GitHub Enterprise Server version 3.7.0 and above and was fixed in version 3.17.19, 3.8.12, 3.9.7 3.10.4, and 3.11.0. **CVE ID : CVE-2023-46646**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2023	4.9	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed arbitrary file reading when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability	N/A	A-GIT-ENTE-160124/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-46645**		
Incorrect Authorization	21-Dec-2023	4.9	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be updated with an improperly scoped token. This vulnerability did not allow unauthorized access to any repository content as it also required contents:write and issues:read permissions. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1.	N/A	A-GIT-ENTE-160124/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51379		
Incorrect Authorization	21-Dec-2023	4.3	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be read with an improperly scoped token. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51380**	N/A	A-GIT-ENTE-160124/176
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	4	A race condition in GitHub Enterprise Server allows an outside collaborator to be added while a repository is being transferred. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6803**	N/A	A-GIT-ENTE-160124/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	2	A race condition in GitHub Enterprise Server allowed an existing admin to maintain permissions on transferred repositories by making a GraphQL mutation to alter repository permissions during the transfer. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6690**	N/A	A-GIT-ENTE-160124/178
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.17.19					
Insertion of Sensitive Information into Log File	21-Dec-2023	5.7	An insertion of sensitive information into log file vulnerability was identified in the log files for a GitHub Enterprise Server back-end service that could permit an `adversary in the middle attack` when combined with other phishing techniques. To exploit this, an attacker would	N/A	A-GIT-ENTE-160124/179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			need access to the log files for the GitHub Enterprise Server appliance, a backup archive created with GitHub Enterprise Server Backup Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6746**		
Authorization Bypass Through User-Controlled Key	21-Dec-2023	5.3	Improper access control in all versions of GitHub Enterprise Server allows unauthorized users to view private repository names via the "Get a check run" API endpoint. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected GitHub Enterprise Server	N/A	A-GIT-ENTE-160124/180

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 3.7.0 and above and was fixed in version 3.17.19, 3.8.12, 3.9.7 3.10.4, and 3.11.0. **CVE ID : CVE-2023-46646**		
Incorrect Authorization	21-Dec-2023	4.9	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be updated with an improperly scoped token. This vulnerability did not allow unauthorized access to any repository content as it also required contents:write and issues:read permissions. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51379**	N/A	A-GIT-ENTE-160124/181
Incorrect Authorization	21-Dec-2023	4.3	An incorrect authorization vulnerability was identified in GitHub Enterprise	N/A	A-GIT-ENTE-160124/182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Server that allowed issue comments to be read with an improperly scoped token. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51380**		
Affected Version(s): From (including) 3.7.0 Up to (excluding) 3.7.19					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	7	A race condition in GitHub Enterprise Server was identified that could allow an attacker administrator access. To exploit this, an organization needs to be converted from a user. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-46649**	N/A	A-GIT-ENTE-160124/183
Improper Limitation of a	21-Dec-2023	4.9	A path traversal vulnerability was identified in	N/A	A-GIT-ENTE-160124/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			GitHub Enterprise Server that allowed arbitrary file reading when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-46645**		
Affected Version(s): From (including) 3.8.0 Up to (excluding) 3.8.12					
Improper Privilege Management	21-Dec-2023	8.8	Improper privilege management in all versions of GitHub Enterprise Server allows users with authorized access to the management console with an editor role to escalate their privileges by making requests to	N/A	A-GIT-ENTE-160124/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the endpoint used for bootstrapping the instance. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.12, 3.9.6, 3.10.3, and 3.11.0. **CVE ID : CVE-2023-46647**		
Insufficient Entropy	21-Dec-2023	7.5	An insufficient entropy vulnerability was identified in GitHub Enterprise Server (GHES) that allowed an attacker to brute force a user invitation to the GHES Management Console. To exploit this vulnerability, an attacker would need knowledge that a user invitation was pending. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	A-GIT-ENTE-160124/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46648		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	7	A race condition in GitHub Enterprise Server was identified that could allow an attacker administrator access. To exploit this, an organization needs to be converted from a user. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-46649**	N/A	A-GIT-ENTE-160124/187
Insertion of Sensitive Information into Log File	21-Dec-2023	6.5	An insertion of sensitive information into the log file in the audit log in GitHub Enterprise Server was identified that could allow an attacker to gain access to the management console. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup	N/A	A-GIT-ENTE-160124/188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			archive created with GitHub Enterprise Server Backup Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6802**		
Insertion of Sensitive Information into Log File	21-Dec-2023	5.7	An insertion of sensitive information into log file vulnerability was identified in the log files for a GitHub Enterprise Server back-end service that could permit an `adversary in the middle attack` when combined with other phishing techniques. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup archive created with GitHub Enterprise Server Backup	N/A	A-GIT-ENTE-160124/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6746**		
Improper Privilege Management	21-Dec-2023	5.5	Improper privilege management allowed arbitrary workflows to be committed and run using an improperly scoped PAT. To exploit this, a workflow must have already existed in the target repo. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6804**	N/A	A-GIT-ENTE-160124/190
Authorization Bypass Through User-	21-Dec-2023	5.3	Improper access control in all versions of GitHub Enterprise Server	N/A	A-GIT-ENTE-160124/191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			allows unauthorized users to view private repository names via the "Get a check run" API endpoint. This vulnerability did not allow unauthorized access to any repository content besides the name. This vulnerability affected GitHub Enterprise Server version 3.7.0 and above and was fixed in version 3.17.19, 3.8.12, 3.9.7 3.10.4, and 3.11.0. **CVE ID : CVE-2023-46646**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2023	4.9	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed arbitrary file reading when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability	N/A	A-GIT-ENTE-160124/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-46645**		
Incorrect Authorization	21-Dec-2023	4.9	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be updated with an improperly scoped token. This vulnerability did not allow unauthorized access to any repository content as it also required contents:write and issues:read permissions. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1.	N/A	A-GIT-ENTE-160124/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51379		
Incorrect Authorization	21-Dec-2023	4.3	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be read with an improperly scoped token. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51380**	N/A	A-GIT-ENTE-160124/194
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	4	A race condition in GitHub Enterprise Server allows an outside collaborator to be added while a repository is being transferred. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6803**	N/A	A-GIT-ENTE-160124/195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	2	A race condition in GitHub Enterprise Server allowed an existing admin to maintain permissions on transferred repositories by making a GraphQL mutation to alter repository permissions during the transfer. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6690**	N/A	A-GIT-ENTE-160124/196
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.6					
Improper Privilege Management	21-Dec-2023	8.8	Improper privilege management in all versions of GitHub Enterprise Server allows users with authorized access to the management console with an editor role to escalate their privileges by making requests to the endpoint used for bootstrapping the instance. This vulnerability affected GitHub Enterprise Server	N/A	A-GIT-ENTE-160124/197

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			version 3.8.0 and above and was fixed in version 3.8.12, 3.9.6, 3.10.3, and 3.11.0. **CVE ID : CVE-2023-46647**		
Affected Version(s): From (including) 3.9.0 Up to (excluding) 3.9.7					
Insufficient Entropy	21-Dec-2023	7.5	An insufficient entropy vulnerability was identified in GitHub Enterprise Server (GHES) that allowed an attacker to brute force a user invitation to the GHES Management Console. To exploit this vulnerability, an attacker would need knowledge that a user invitation was pending. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-46648**	N/A	A-GIT-ENTE-160124/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	21-Dec-2023	7.5	An improper authentication vulnerability was identified in GitHub Enterprise Server that allowed a bypass of Private Mode by using a specially crafted API request. To exploit this vulnerability, an attacker would need network access to the Enterprise Server appliance configured in Private Mode. This vulnerability affected all versions of GitHub Enterprise Server since 3.9 and was fixed in version 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program. **CVE ID : CVE-2023-6847**	N/A	A-GIT-ENTE-160124/199
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	7	A race condition in GitHub Enterprise Server was identified that could allow an attacker administrator access. To exploit this, an	N/A	A-GIT-ENTE-160124/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			organization needs to be converted from a user. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-46649**		
Insertion of Sensitive Information into Log File	21-Dec-2023	6.5	An insertion of sensitive information into the log file in the audit log in GitHub Enterprise Server was identified that could allow an attacker to gain access to the management console. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup archive created with GitHub Enterprise Server Backup Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was	N/A	A-GIT-ENTE-160124/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6802**		
Insertion of Sensitive Information into Log File	21-Dec-2023	5.7	An insertion of sensitive information into log file vulnerability was identified in the log files for a GitHub Enterprise Server back-end service that could permit an `adversary in the middle attack` when combined with other phishing techniques. To exploit this, an attacker would need access to the log files for the GitHub Enterprise Server appliance, a backup archive created with GitHub Enterprise Server Backup Utilities, or a service which received streamed logs. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12,	N/A	A-GIT-ENTE-160124/202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6746**		
Improper Privilege Management	21-Dec-2023	5.5	Improper privilege management allowed arbitrary workflows to be committed and run using an improperly scoped PAT. To exploit this, a workflow must have already existed in the target repo. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6804**	N/A	A-GIT-ENTE-160124/203
Authorization Bypass Through User-Controlled Key	21-Dec-2023	5.3	Improper access control in all versions of GitHub Enterprise Server allows unauthorized users to view private repository names via the "Get a check run" API endpoint. This vulnerability did not allow unauthorized access to any repository content	N/A	A-GIT-ENTE-160124/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			besides the name. This vulnerability affected GitHub Enterprise Server version 3.7.0 and above and was fixed in version 3.17.19, 3.8.12, 3.9.7 3.10.4, and 3.11.0. **CVE ID : CVE-2023-46646**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2023	4.9	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed arbitrary file reading when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.7.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. This vulnerability was reported via the GitHub Bug Bounty program.	N/A	A-GIT-ENTE-160124/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46645		
Incorrect Authorization	21-Dec-2023	4.9	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be updated with an improperly scoped token. This vulnerability did not allow unauthorized access to any repository content as it also required contents:write and issues:read permissions. This vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51379**	N/A	A-GIT-ENTE-160124/206
Incorrect Authorization	21-Dec-2023	4.3	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed issue comments to be read with an improperly scoped token. This	N/A	A-GIT-ENTE-160124/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affected all versions of GitHub Enterprise Server since 3.7 and was fixed in version 3.17.19, 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-51380**		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	4	A race condition in GitHub Enterprise Server allows an outside collaborator to be added while a repository is being transferred. This vulnerability affected all versions of GitHub Enterprise Server since 3.8 and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6803**	N/A	A-GIT-ENTE-160124/208
Time-of-check Time-of-use (TOCTOU) Race Condition	21-Dec-2023	2	A race condition in GitHub Enterprise Server allowed an existing admin to maintain permissions on transferred repositories by making a GraphQL mutation to alter repository permissions during	N/A	A-GIT-ENTE-160124/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the transfer. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.12, 3.9.7, 3.10.4, and 3.11.1. **CVE ID : CVE-2023-6690**		
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): From (including) 16.0.0 Up to (excluding) 16.4.4					
Improper Privilege Management	17-Dec-2023	8.8	A privilege escalation vulnerability in GitLab EE affecting all versions from 16.0 prior to 16.4.4, 16.5 prior to 16.5.4, and 16.6 prior to 16.6.2 allows a project Maintainer to use a Project Access Token to escalate their role to Owner **CVE ID : CVE-2023-3907**	N/A	A-GIT-GITL-160124/210
Affected Version(s): From (including) 16.5 Up to (excluding) 16.5.4					
Improper Privilege Management	17-Dec-2023	8.8	A privilege escalation vulnerability in GitLab EE affecting all versions from 16.0 prior to 16.4.4, 16.5 prior to 16.5.4, and 16.6 prior to 16.6.2	N/A	A-GIT-GITL-160124/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a project Maintainer to use a Project Access Token to escalate their role to Owner **CVE ID : CVE-2023-3907**		
Affected Version(s): From (including) 16.6 Up to (excluding) 16.6.2					
Improper Privilege Management	17-Dec-2023	8.8	A privilege escalation vulnerability in GitLab EE affecting all versions from 16.0 prior to 16.4.4, 16.5 prior to 16.5.4, and 16.6 prior to 16.6.2 allows a project Maintainer to use a Project Access Token to escalate their role to Owner **CVE ID : CVE-2023-3907**	N/A	A-GIT-GITL-160124/212
Vendor: glensawyer					
Product: mp3gain					
Affected Version(s): 1.6.2					
Out-of-bounds Write	22-Dec-2023	7.5	A stack buffer overflow vulnerability in MP3Gain v1.6.2 allows an attacker to cause a denial of service via the WriteMP3GainAPETag function at apetag.c:592. **CVE ID : CVE-2023-49356**	N/A	A-GLE-MP3G-160124/213
Vendor: Golang					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: crypto					
Affected Version(s): * Up to (excluding) 0.17.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-GOL-CRYP-160124/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Google					
Product: chrome					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 120.0.6099.129					
Out-of-bounds Write	21-Dec-2023	8.8	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-7024**	https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html	A-GOO-CHRO-160124/215
Vendor: gopiplus					
Product: image_horizontal_reel_scroll_slideshow					
Affected Version(s): * Up to (including) 13.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2023	5.4	The Image horizontal reel scroll slideshow plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'ihrss-gallery' shortcode in versions up to, and including, 13.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to	https://plugins.trac.wordpress.org/changeset/3010834/image-horizontal-reel-scroll-slideshow	A-GOP-IMAG-160124/216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5413**		
Product: jquery_news_ticker					
Affected Version(s): * Up to (including) 3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2023	5.4	The Jquery news ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'jquery-news-ticker' shortcode in versions up to, and including, 3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-5432**	https://plugins.trac.wordpress.org/changeset/3010828/jquery-news-ticker	A-GOP-JQUE-160124/217
Vendor: gravityforms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: gravity_forms					
Affected Version(s): * Up to (excluding) 2.7.4					
Deserialization of Untrusted Data	20-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in Rocketgenius Inc. Gravity Forms.This issue affects Gravity Forms: from n/a through 2.7.3. **CVE ID : CVE-2023-28782**	N/A	A-GRA-GRAV-160124/218
Vendor: gravitymaster					
Product: product_enquiry_for_woocommerce					
Affected Version(s): * Up to (including) 3.0					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Gravity Master Product Enquiry for WooCommerce.This issue affects Product Enquiry for WooCommerce: from n/a through 3.0. **CVE ID : CVE-2023-49761**	N/A	A-GRA-PROD-160124/219
Vendor: guardgiant					
Product: guardgiant					
Affected Version(s): * Up to (including) 2.2.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GuardGiant Brute Force Protection WordPress Brute Force Protection – Stop Brute Force Attacks.This issue affects WordPress Brute Force Protection – Stop Brute Force Attacks: from n/a through 2.2.5. **CVE ID : CVE-2023-48764**	N/A	A-GUA-GUAR-160124/220
Vendor: guelbetech					
Product: bravo_translate					
Affected Version(s): * Up to (including) 1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Guelben Bravo Translate.This issue affects Bravo Translate: from n/a through 1.2.	N/A	A-GUE-BRAV-160124/221

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49161		
Vendor: gvectors					
Product: woodiscuz_-_woocommerce_comments					
Affected Version(s): * Up to (including) 2.3.0					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in gVectors Team WooDiscuz – WooCommerce Comments.This issue affects WooDiscuz – WooCommerce Comments: from n/a through 2.3.0. **CVE ID : CVE-2023-49759**	N/A	A-GVE-WOOD-160124/222
Product: wpdiscuz					
Affected Version(s): * Up to (excluding) 7.6.4					
Authorization Bypass Through User-Controlled Key	20-Dec-2023	6.5	Authorization Bypass Through User-Controlled Key vulnerability in gVectors Team Comments – wpDiscuz.This issue affects Comments – wpDiscuz: from n/a through 7.6.3. **CVE ID : CVE-2023-46311**	N/A	A-GVE-WPDI-160124/223
Vendor: gvnpatidar					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: hotel_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Hotel Management v1.0 is vulnerable to multiple authenticated Reflected Cross-Site Scripting vulnerabilities. The 'adults' parameter of the reservation.php resource is copied into the HTML document as plain text between tags. Any input is echoed unmodified in the application's response. **CVE ID : CVE-2023-49269**	N/A	A-GVN-HOTE-160124/224
Vendor: halgatewood					
Product: dashicons_\+_custom_post_types					
Affected Version(s): * Up to (including) 1.0.2					
Cross-Site Request Forgery (CSRF)	21-Dec-2023	8.8	Missing Authorization, Cross-Site Request Forgery (CSRF) vulnerability in Hal Gatewood Dashicons + Custom Post Types.This issue affects Dashicons + Custom Post Types: from n/a through 1.0.2.	N/A	A-HAL-DASH-160124/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22674		
Vendor: hcltech					
Product: bigfix_modern_client_management					
Affected Version(s): * Up to (excluding) 3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	4.8	Due to this vulnerability, the Master operator could potentially incorporate an SVG tag into HTML, leading to an alert pop-up displaying a cookie. To mitigate stored XSS vulnerabilities, a preventive measure involves thoroughly sanitizing and validating all user inputs before they are processed and stored in the server storage. **CVE ID : CVE-2023-28025**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109318	A-HCL-BIGF-160124/226
Product: bigfix_platform					
Affected Version(s): 11.0.0					
Improper Neutralization of Input During Web Page Generation	21-Dec-2023	6.1	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability. This XSS vulnerability is in the Download Status Report,	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109376	A-HCL-BIGF-160124/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			which is served by the BigFix Server. **CVE ID : CVE-2023-37519**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	6.1	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability identified in BigFix Server version 9.5.12.68, allowing for potential data exfiltration. This XSS vulnerability is in the Gather Status Report, which is served by the BigFix Relay. **CVE ID : CVE-2023-37520**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109376	A-HCL-BIGF-160124/228
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	6.1	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability. This XSS vulnerability is in the Download Status Report, which is served by the BigFix Server. **CVE ID : CVE-2023-37519**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109376	A-HCL-BIGF-160124/229
Improper Neutralization of Input During Web Page	21-Dec-2023	6.1	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability identified in BigFix Server version	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109376	A-HCL-BIGF-160124/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			9.5.12.68, allowing for potential data exfiltration. This XSS vulnerability is in the Gather Status Report, which is served by the BigFix Relay. **CVE ID : CVE-2023-37520**		
Affected Version(s): From (including) 9.5 Up to (excluding) 9.5.23					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	6.1	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability. This XSS vulnerability is in the Download Status Report, which is served by the BigFix Server. **CVE ID : CVE-2023-37519**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109376	A-HCL-BIGF-160124/231
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	6.1	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability identified in BigFix Server version 9.5.12.68, allowing for potential data exfiltration. This XSS vulnerability is in the Gather Status Report, which is served by the BigFix Relay. **CVE ID : CVE-2023-37520**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0109376	A-HCL-BIGF-160124/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: heimdalsecurity					
Product: thor					
Affected Version(s): * Up to (excluding) 3.7.0					
N/A	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before 3.7.0 on Windows, allows attackers to bypass USB access restrictions, execute arbitrary code, and obtain sensitive information via Next-Gen Antivirus component. **CVE ID : CVE-2023-29486**	N/A	A-HEI-THOR-160124/233
Affected Version(s): * Up to (including) 2.6.9					
Missing Authentication for Critical Function	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before on Windows and 2.6.9 and before on macOS, allows attackers to bypass network filtering, execute arbitrary code, and obtain sensitive information via DarkLayer Guard threat prevention module. **CVE ID : CVE-2023-29485**	N/A	A-HEI-THOR-160124/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before 3.7.0 on Windows, allows attackers to bypass USB access restrictions, execute arbitrary code, and obtain sensitive information via Next-Gen Antivirus component. **CVE ID : CVE-2023-29486**	N/A	A-HEI-THOR-160124/235
Affected Version(s): * Up to (including) 3.5.3					
Missing Authentication for Critical Function	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before on Windows and 2.6.9 and before on macOS, allows attackers to bypass network filtering, execute arbitrary code, and obtain sensitive information via DarkLayer Guard threat prevention module. **CVE ID : CVE-2023-29485**	N/A	A-HEI-THOR-160124/236
Vendor: hitachienergy					
Product: rtu500_scripting_interface					
Affected Version(s): 1.0.1.30					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	19-Dec-2023	7.5	A vulnerability exists in the component RTU500 Scripting interface. When a client connects to a server using TLS, the server presents a certificate. This certificate links a public key to the identity of the service and is signed by a Certification Authority (CA), allowing the client to validate that the remote service can be trusted and is not malicious. If the client does not validate the parameters of the certificate, then attackers could be able to spoof the identity of the service. An attacker could exploit the vulnerability by using faking the identity of a RTU500 device and intercepting the messages initiated via the RTU500 Scripting interface. **CVE ID : CVE-2023-1514**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000152&languageCode=en&Preview=true	A-HIT-RTU5-160124/237
Affected Version(s): 1.0.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	19-Dec-2023	7.5	A vulnerability exists in the component RTU500 Scripting interface. When a client connects to a server using TLS, the server presents a certificate. This certificate links a public key to the identity of the service and is signed by a Certification Authority (CA), allowing the client to validate that the remote service can be trusted and is not malicious. If the client does not validate the parameters of the certificate, then attackers could be able to spoof the identity of the service. An attacker could exploit the vulnerability by using faking the identity of a RTU500 device and intercepting the messages initiated via the RTU500 Scripting interface. **CVE ID : CVE-2023-1514**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000152&languageCode=en&Preview=true	A-HIT-RTU5-160124/238
Affected Version(s): 1.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	19-Dec-2023	7.5	A vulnerability exists in the component RTU500 Scripting interface. When a client connects to a server using TLS, the server presents a certificate. This certificate links a public key to the identity of the service and is signed by a Certification Authority (CA), allowing the client to validate that the remote service can be trusted and is not malicious. If the client does not validate the parameters of the certificate, then attackers could be able to spoof the identity of the service. An attacker could exploit the vulnerability by using faking the identity of a RTU500 device and intercepting the messages initiated via the RTU500 Scripting interface. **CVE ID : CVE-2023-1514**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000152&languageCode=en&Preview=true	A-HIT-RTU5-160124/239
Vendor: hmplugin					
Product: jobwp					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 2.0					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in HM Plugin WordPress Job Board and Recruitment Plugin – JobWP.This issue affects WordPress Job Board and Recruitment Plugin – JobWP: from n/a through 2.0. **CVE ID : CVE-2023-29384**	N/A	A-HMP-JOBW-160124/240
Affected Version(s): * Up to (excluding) 2.2					
Exposure of Sensitive Information to an Unauthorized Actor	21-Dec-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in HM Plugin WordPress Job Board and Recruitment Plugin – JobWP.This issue affects WordPress Job Board and Recruitment Plugin – JobWP: from n/a through 2.1. **CVE ID : CVE-2023-48288**	N/A	A-HMP-JOBW-160124/241
Vendor: HP					
Product: system_management_homepage					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) a.3.2.23.09					
N/A	17-Dec-2023	7.5	A potential security vulnerability has been identified with HP-UX System Management Homepage (SMH). This vulnerability could be exploited locally or remotely to disclose information. **CVE ID : CVE-2023-50271**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04551en_us	A-HP-SYST-160124/242
Vendor: huggingface					
Product: transformers					
Affected Version(s): * Up to (excluding) 4.36.0					
Deserialization of Untrusted Data	19-Dec-2023	8.8	Deserialization of Untrusted Data in GitHub repository huggingface/transformers prior to 4.36. **CVE ID : CVE-2023-6730**	https://github.com/huggingface/transformers/commit/1d63b0ec361e7a38f1339385e8a5a855085532ce	A-HUG-TRAN-160124/243
Deserialization of Untrusted Data	20-Dec-2023	7.8	Deserialization of Untrusted Data in GitHub repository huggingface/transformers prior to 4.36. **CVE ID : CVE-2023-7018**	https://huntr.com/bounties/e1a3e548-e53a-48df-b708-9ee62140963c, https://github.com/huggingface/transformers/commit/1d63b0ec361e7a38f1339385e8a5a855085532ce	A-HUG-TRAN-160124/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: IBM					
Product: cloud_pak_for_business_automation					
Affected Version(s): 18.0.0					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/245
Affected Version(s): 18.0.2					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**		
Affected Version(s): 19.0.1					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/247
Affected Version(s): 19.0.3					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**		
Affected Version(s): 20.0.1					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/249
Affected Version(s): 20.0.3					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**		
Affected Version(s): 21.0.1					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/251
Affected Version(s): 21.0.3					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**		
Affected Version(s): 22.0.2					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/253
Affected Version(s): 23.0.1					
N/A	18-Dec-2023	4.9	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and	https://www.ibm.com/support/pages/node/7096365, https://exchange.xforce.ibmcloud.com/vulnerabilities/264805	A-IBM-CLOU-160124/254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805. **CVE ID : CVE-2023-40691**		
Product: db2_mirror_for_i					
Affected Version(s): 7.4					
Insufficiently Protected Credentials	18-Dec-2023	5.3	IBM i 7.3, 7.4, 7.5, IBM i Db2 Mirror for i 7.4 and 7.5 web browser clients may leave clear-text passwords in browser memory that can be viewed using common browser tools before the memory is garbage collected. A malicious actor with access to the victim's PC could exploit this vulnerability to gain access to the IBM i operating system. IBM X-Force ID: 272532.	https://www.ibm.com/support/pages/node/7097785, https://www.ibm.com/support/pages/node/7097801	A-IBM-DB2_-160124/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47741		
Affected Version(s): 7.5					
Insufficiently Protected Credentials	18-Dec-2023	5.3	IBM i 7.3, 7.4, 7.5, IBM i Db2 Mirror for i 7.4 and 7.5 web browser clients may leave clear-text passwords in browser memory that can be viewed using common browser tools before the memory is garbage collected. A malicious actor with access to the victim's PC could exploit this vulnerability to gain access to the IBM i operating system. IBM X-Force ID: 272532. **CVE ID : CVE-2023-47741**	https://www.ibm.com/support/pages/node/7097785, https://www.ibm.com/support/pages/node/7097801	A-IBM-DB2_-160124/256
Product: i					
Affected Version(s): 7.4					
Insufficiently Protected Credentials	18-Dec-2023	5.3	IBM i 7.3, 7.4, 7.5, IBM i Db2 Mirror for i 7.4 and 7.5 web browser clients may leave clear-text passwords in	https://www.ibm.com/support/pages/node/7097785, https://www.ibm.com/support/pages/node/7097801	A-IBM-I-160124/257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			browser memory that can be viewed using common browser tools before the memory is garbage collected. A malicious actor with access to the victim's PC could exploit this vulnerability to gain access to the IBM i operating system. IBM X-Force ID: 272532. **CVE ID : CVE-2023-47741**		
Affected Version(s): 7.5					
Insufficiently Protected Credentials	18-Dec-2023	5.3	IBM i 7.3, 7.4, 7.5, IBM i Db2 Mirror for i 7.4 and 7.5 web browser clients may leave clear-text passwords in browser memory that can be viewed using common browser tools before the memory is garbage collected. A malicious actor with access to the victim's PC could exploit this vulnerability to gain access to the	https://www.ibm.com/support/pages/node/7097785, https://www.ibm.com/support/pages/node/7097801	A-IBM-I-160124/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM i operating system. IBM X-Force ID: 272532. **CVE ID : CVE-2023-47741**		
Affected Version(s): 7.3					
Insufficiently Protected Credentials	18-Dec-2023	5.3	IBM i 7.3, 7.4, 7.5, IBM i Db2 Mirror for i 7.4 and 7.5 web browser clients may leave clear-text passwords in browser memory that can be viewed using common browser tools before the memory is garbage collected. A malicious actor with access to the victim's PC could exploit this vulnerability to gain access to the IBM i operating system. IBM X-Force ID: 272532. **CVE ID : CVE-2023-47741**	https://www.ibm.com/support/pages/node/7097785, https://www.ibm.com/support/pages/node/7097801	A-IBM-I-160124/259
Product: informix_jdbc					
Affected Version(s): 4.10					
Improper Neutralizat	20-Dec-2023	9.8	IBM Informix JDBC Driver 4.10 and	https://www.ibm.com/support	A-IBM-INFO-160124/260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements in Output Used by a Downstream Component ('Injection')			4.50 is susceptible to remote code execution attack via JNDI injection when passing an unchecked argument to a certain API. IBM X-Force ID: 259116. **CVE ID : CVE-2023-35895**	/pages/node/7099762, https://exchange.xforce.ibmcloud.com/vulnerabilities/259116	
Affected Version(s): 4.50					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Dec-2023	9.8	IBM Informix JDBC Driver 4.10 and 4.50 is susceptible to remote code execution attack via JNDI injection when passing an unchecked argument to a certain API. IBM X-Force ID: 259116. **CVE ID : CVE-2023-35895**	https://www.ibm.com/support/pages/node/7099762, https://exchange.xforce.ibmcloud.com/vulnerabilities/259116	A-IBM-INFO-160124/261
Product: mq_appliance					
Affected Version(s): 9.3.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	7.5	IBM MQ Appliance 9.3 LTS and 9.3 CD could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request to view arbitrary files on the system. IBM X-Force ID: 269536.	https://www.ibm.com/support/pages/node/7091235, https://exchange.xforce.ibmcloud.com/vulnerabilities/269536	A-IBM-MQ_A-160124/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46177		
Product: planning_analytics					
Affected Version(s): 2.0					
Unrestricted Upload of File with Dangerous Type	22-Dec-2023	9.8	IBM Planning Analytics Local 2.0 could allow a remote attacker to upload arbitrary files, caused by the improper validation of file extensions. By sending a specially crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious script, which could allow the attacker to execute arbitrary code on the vulnerable system. IBM X-Force ID: 265567. **CVE ID : CVE-2023-42017**	https://www.ibm.com/support/pages/node/7096528, https://exchange.xforce.ibmcloud.com/vulnerabilities/265567	A-IBM-PLAN-160124/263
Product: qradar_security_information_and_event_manager					
Affected Version(s): 7.5.0					
N/A	19-Dec-2023	6.5	IBM Qradar SIEM 7.5 could allow a privileged user to obtain sensitive domain information due to data being misidentified. IBM X-Force ID: 270372.	https://https://www.ibm.com/support/pages/node/7099297, https://exchange.xforce.ibmcloud.com/vulnerabilities/270372	A-IBM-QRAD-160124/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47146		
Product: security_guardium_key_lifecycle_manager					
Affected Version(s): From (including) 4.2.0 Up to (excluding) 4.2.0.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2023	9.1	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view modify files on the system. IBM X-Force ID: 271196. **CVE ID : CVE-2023-47702**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271196	A-IBM-SECU-160124/265
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to upload files of a dangerous file type. IBM X-Force ID: 271341. **CVE ID : CVE-2023-47706**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271341	A-IBM-SECU-160124/266
Use of Hard-coded Credentials	20-Dec-2023	7.5	IBM Security Guardium Key Lifecycle Manager 4.3 contains plain text hard-coded credentials or other secrets in source code	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud	A-IBM-SECU-160124/267

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			repository. IBM X-Force ID: 271220. **CVE ID : CVE-2023-47704**	d.com/vulnerabilities/271220	
Generation of Error Message Containing Sensitive Information	20-Dec-2023	5.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 271197. **CVE ID : CVE-2023-47703**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271197	A-IBM-SECU-160124/268
Improper Input Validation	20-Dec-2023	4.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to manipulate username data due to improper input validation. IBM X-Force ID: 271228. **CVE ID : CVE-2023-47705**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271228	A-IBM-SECU-160124/269
Affected Version(s): From (including) 4.2.0 Up to (including) 4.2.0.2					
Improper Neutralization of Input During Web Page Generation	20-Dec-2023	5.4	IBM Security Guardium Key Lifecycle Manager 4.3 is vulnerable to cross-site scripting. This vulnerability allows users to	https://www.ibm.com/support/pages/node/7091157	A-IBM-SECU-160124/270

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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: 271522. **CVE ID : CVE-2023-47707**		
Product: urbancode_deploy					
Affected Version(s): From (including) 7.0.0.0 Up to (including) 7.0.5.18					
Improper Input Validation	20-Dec-2023	6.5	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 may mishandle input validation of an uploaded archive file leading to a denial of service due to resource exhaustion. IBM X-Force ID: 270799. **CVE ID : CVE-2023-47161**	https://www.ibm.com/support/pages/node/7096552	A-IBM-URBA-160124/271
Generation of Error Message Containing Sensitive Information	20-Dec-2023	5.3	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 could allow a remote attacker to obtain sensitive information when a detailed technical	https://www.ibm.com/support/pages/node/7096547	A-IBM-URBA-160124/272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 265510. **CVE ID : CVE-2023-42013**		
Affected Version(s): From (including) 7.1.0.0 Up to (excluding) 7.1.2.15					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2023	4.3	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 is vulnerable to HTML injection. This vulnerability may allow a user to embed arbitrary HTML tags in the Web UI potentially leading to sensitive information disclosure. IBM X-Force ID: 265512. **CVE ID : CVE-2023-42015**	https://www.ibm.com/support/pages/node/7096546, https://exchange.xforce.ibmcloud.com/vulnerabilities/265512	A-IBM-URBA-160124/273
Affected Version(s): From (including) 7.1.0.0 Up to (including) 7.1.2.14					
Improper Input Validation	20-Dec-2023	6.5	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 may mishandle input validation of an uploaded archive file leading to a denial of service	https://www.ibm.com/support/pages/node/7096552	A-IBM-URBA-160124/274

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to resource exhaustion. IBM X-Force ID: 270799. **CVE ID : CVE-2023-47161**		
Generation of Error Message Containing Sensitive Information	20-Dec-2023	5.3	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 265510. **CVE ID : CVE-2023-42013**	https://www.ibm.com/support/pages/node/7096547	A-IBM-URBA-160124/275
Affected Version(s): From (including) 7.2.0.0 Up to (excluding) 7.2.3.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2023	4.3	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 is vulnerable to HTML injection. This vulnerability may allow a user to embed arbitrary HTML tags in the Web UI potentially leading to sensitive information	https://www.ibm.com/support/pages/node/7096546, https://exchange.xforce.ibmcloud.com/vulnerabilities/265512	A-IBM-URBA-160124/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure. IBM X-Force ID: 265512. **CVE ID : CVE-2023-42015**		
Affected Version(s): From (including) 7.2.0.0 Up to (including) 7.2.3.7					
Improper Input Validation	20-Dec-2023	6.5	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 may mishandle input validation of an uploaded archive file leading to a denial of service due to resource exhaustion. IBM X-Force ID: 270799. **CVE ID : CVE-2023-47161**	https://www.ibm.com/support/pages/node/7096552	A-IBM-URBA-160124/277
N/A	20-Dec-2023	5.5	An IBM UrbanCode Deploy Agent 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 installed as a Windows service in a non-standard location could be subject to a denial of service attack by local accounts. IBM X-Force ID: 265509. **CVE ID : CVE-2023-42012**	https://www.ibm.com/support/pages/node/7096548	A-IBM-URBA-160124/278
Generation of Error Message Containing Sensitive	20-Dec-2023	5.3	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 could allow	https://www.ibm.com/support/pages/node/7096547	A-IBM-URBA-160124/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 265510. **CVE ID : CVE-2023-42013**		
Affected Version(s): From (including) 7.3.0.0 Up to (excluding) 7.3.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2023	4.3	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 is vulnerable to HTML injection. This vulnerability may allow a user to embed arbitrary HTML tags in the Web UI potentially leading to sensitive information disclosure. IBM X-Force ID: 265512. **CVE ID : CVE-2023-42015**	https://www.ibm.com/support/pages/node/7096546, https://exchange.xforce.ibmcloud.com/vulnerabilities/265512	A-IBM-URBA-160124/280
Affected Version(s): From (including) 7.3.0.0 Up to (including) 7.3.2.2					
Improper Input Validation	20-Dec-2023	6.5	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 may mishandle input	https://www.ibm.com/support/pages/node/7096552	A-IBM-URBA-160124/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of an uploaded archive file leading to a denial of service due to resource exhaustion. IBM X-Force ID: 270799. **CVE ID : CVE-2023-47161**		
N/A	20-Dec-2023	5.5	An IBM UrbanCode Deploy Agent 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 installed as a Windows service in a non-standard location could be subject to a denial of service attack by local accounts. IBM X-Force ID: 265509. **CVE ID : CVE-2023-42012**	https://www.ibm.com/support/pages/node/7096548	A-IBM-URBA-160124/282
Generation of Error Message Containing Sensitive Information	20-Dec-2023	5.3	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 265510.	https://www.ibm.com/support/pages/node/7096547	A-IBM-URBA-160124/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-42013		
Product: vios					
Affected Version(s): 3.1					
N/A	19-Dec-2023	5.5	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in AIX windows to cause a denial of service. IBM X-Force ID: 267970. **CVE ID : CVE-2023-45172**	https://www.ibm.com/support/pages/node/7099314, https://exchange.xforce.ibmcloud.com/vulnerabilities/267970	A-IBM-VIOS-160124/284
Vendor: imoulife					
Product: imou_life					
Affected Version(s): 6.7.0					
Session Fixation	19-Dec-2023	8.1	A session hijacking vulnerability has been detected in the Imou Life application affecting version 6.7.0. This vulnerability could allow an attacker to hijack user accounts due to the QR code functionality not properly filtering codes when scanning a new device and directly running WebView without prompting or displaying it to the user. This vulnerability could	N/A	A-IMO-IMOU-160124/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trigger phishing attacks. **CVE ID : CVE-2023-6913**		
Vendor: infinispan					
Product: infinispan					
Affected Version(s): -					
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST. Bulk read endpoints do not properly evaluate user permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions. **CVE ID : CVE-2023-3628**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-3628	A-INF-INFI-160124/286
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST, Cache retrieval endpoints do not properly evaluate the necessary admin permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions.	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-3629	A-INF-INFI-160124/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-3629		
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan, which does not detect circular object references when unmarshalling. An authenticated attacker with sufficient permissions could insert a maliciously constructed object into the cache and use it to cause out of memory errors and achieve a denial of service. **CVE ID : CVE-2023-5236**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-5236	A-INF-INFI-160124/288
Cleartext Storage of Sensitive Information	18-Dec-2023	2.7	A flaw was found in Infinispan. When serializing the configuration for a cache to XML/JSON/YAML, which contains credentials (JDBC store with connection pooling, remote store), the credentials are returned in clear text as part of the configuration. **CVE ID : CVE-2023-5384**	https://access.redhat.com/errata/RHSA-2023:7676, https://access.redhat.com/security/cve/CVE-2023-5384	A-INF-INFI-160124/289
Vendor: ipages_flipbook_project					
Product: ipages_flipbook					
Affected Version(s): * Up to (excluding) 1.5.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	4.9	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Avirtum iPages Flipbook For WordPress.This issue affects iPages Flipbook For WordPress: from n/a through 1.4.8. **CVE ID : CVE-2023-47236**	N/A	A-IPA-IPAG-160124/290
Vendor: iscute					
Product: cute_http_file_server					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Cross Site Scripting (XSS) vulnerability in CuteHttpFileServer v.1.0 and v.2.0 allows attackers to obtain sensitive information via the file upload function in the home page. **CVE ID : CVE-2023-50639**	N/A	A-ISC-CUTE-160124/291
Affected Version(s): 2.0					
Improper Neutralization of Input During Web Page Generation	20-Dec-2023	5.4	Cross Site Scripting (XSS) vulnerability in CuteHttpFileServer v.1.0 and v.2.0 allows attackers to obtain sensitive	N/A	A-ISC-CUTE-160124/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			information via the file upload function in the home page. **CVE ID : CVE-2023-50639**		
Vendor: iteachyou					
Product: dreamer_cms					
Affected Version(s): 4.1.3					
Unrestricted Upload of File with Dangerous Type	24-Dec-2023	8.8	A vulnerability was found in Dreamer CMS 4.1.3. It has been declared as problematic. This vulnerability affects unknown code of the file /upload/uploadFile. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-248938 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-2023-7091**	N/A	A-ITE-DREA-160124/293
Vendor: ivanti					
Product: avalanche					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 6.4.2					
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-41727**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/294
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46216**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/295
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46217		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46220**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/297
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46221**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/298
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46222		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46223**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/300
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46224**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/301
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46225		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46257**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/303
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46258**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/304
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46259		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46260**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/306
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46261**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/307
Unrestricted Upload of File with Dangerous Type	19-Dec-2023	9.8	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remote code execution. **CVE ID : CVE-2023-46263**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	19-Dec-2023	9.8	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remove code execution. **CVE ID : CVE-2023-46264**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/309
Out-of-bounds Write	19-Dec-2023	7.5	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS). **CVE ID : CVE-2023-46803**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/310
Out-of-bounds Write	19-Dec-2023	7.5	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS). **CVE ID : CVE-2023-46804**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	A-IVA-AVAL-160124/311
Affected Version(s): * Up to (including) 6.4.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	19-Dec-2023	9.8	An unauthenticated could abuse a XXE vulnerability in the Smart Device Server to leak data or perform a Server-Side Request Forgery (SSRF). **CVE ID : CVE-2023-46265**	N/A	A-IVA-AVAL-160124/312
N/A	19-Dec-2023	9.1	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack. **CVE ID : CVE-2023-46266**	N/A	A-IVA-AVAL-160124/313
Server-Side Request Forgery (SSRF)	19-Dec-2023	7.5	An unauthenticated attacked could send a specially crafted web request causing a Server-Side Request Forgery (SSRF) in Ivanti Avalanche Remote Control server. **CVE ID : CVE-2023-46262**	N/A	A-IVA-AVAL-160124/314
Product: connect_secure					
Affected Version(s): -					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure	https://forums.ivanti.com/s/article/Security-fix-release-	A-IVA-CONN-160124/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	
Affected Version(s): 21.12					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	https://forums.ivanti.com/s/article/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	A-IVA-CONN-160124/316
Affected Version(s): 21.9					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	https://forums.ivanti.com/s/article/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	A-IVA-CONN-160124/317
Affected Version(s): 22.1					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti	https://forums.ivanti.com/s/article/Security-	A-IVA-CONN-160124/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	
Affected Version(s): 22.2					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	https://forums.ivanti.com/s/article/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	A-IVA-CONN-160124/319
Affected Version(s): 22.3					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	https://forums.ivanti.com/s/article/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	A-IVA-CONN-160124/320
Affected Version(s): 22.4					
N/A	16-Dec-2023	7.5	A vulnerability exists on all	https://forums.ivanti.com/s/art	A-IVA-CONN-160124/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	icle/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	
Affected Version(s): 22.5					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	https://forums.ivanti.com/s/article/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	A-IVA-CONN-160124/322
Affected Version(s): 22.6					
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	https://forums.ivanti.com/s/article/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	A-IVA-CONN-160124/323
Affected Version(s): 9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Dec-2023	7.5	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. **CVE ID : CVE-2023-39340**	https://forums.ivanti.com/s/article/Security-fix-release-Ivanti-Connect-Secure-22-6R2-and-22-6R2-1?language=en_US	A-IVA-CONN-160124/324
Vendor: jacksonwhelan					
Product: iframe_shortcode					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Terrier Tenacity iframe Shortcode allows Stored XSS.This issue affects iframe Shortcode: from n/a through 2.0. **CVE ID : CVE-2023-50825**	N/A	A-JAC-IFRA-160124/325
Vendor: jadaptive					
Product: maverick_synergy_java_ssh_api					
Affected Version(s): * Up to (excluding) 3.1.0-snapshot					
Improper Validation of Integrity	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH	https://github.com/openssh/openssh-	A-JAD-MAVE-160124/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Check Value			extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC	portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Jetbrains					
Product: intellij_idea					
Affected Version(s): * Up to (excluding) 2023.3.2					
Insufficient Verification of Data	21-Dec-2023	9.8	In JetBrains IntelliJ IDEA before 2023.3.2 code execution was	https://www.jetbrains.com/privacy-	A-JET-INTE-160124/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			possible in Untrusted Project mode via a malicious plugin repository specified in the project configuration **CVE ID : CVE-2023-51655**	security/issues-fixed/	
Vendor: kainelabs					
Product: youzify					
Affected Version(s): * Up to (excluding) 1.2.3					
Authorization Bypass Through User-Controlled Key	21-Dec-2023	6.5	Authorization Bypass Through User-Controlled Key vulnerability in KaineLabs Youzify – BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress.This issue affects Youzify – BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress: from n/a through 1.2.2. **CVE ID : CVE-2023-47191**	N/A	A-KAI-YOUZ-160124/328
Vendor: kakadusoftware					
Product: kakadu_sdk					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.4 Up to (including) 8.4					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	7.5	JPX Fragment List (flst) box vulnerability in Kakadu 7.9 allows an attacker to exfiltrate local and remote files reachable by a server if the server allows the attacker to upload a specially-crafted the image that is displayed back to the attacker. **CVE ID : CVE-2023-6562**	N/A	A-KAK-KAKA-160124/329
Vendor: kashipara					
Product: hotel_management					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	6.1	Hotel Management v1.0 is vulnerable to multiple authenticated Reflected Cross-Site Scripting vulnerabilities. The 'children' parameter of the reservation.php resource is copied into the HTML document as plain text between tags. Any input is echoed unmodified in the application's response.	N/A	A-KAS-HOTE-160124/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49272		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Hotel Management v1.0 is vulnerable to multiple authenticated Reflected Cross-Site Scripting vulnerabilities. The 'check_in_date' parameter of the reservation.php resource is copied into the HTML document as plain text between tags. Any input is echoed unmodified in the application's response. **CVE ID : CVE-2023-49270**	https://www.kashipara.com/	A-KAS-HOTE-160124/331
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	Hotel Management v1.0 is vulnerable to multiple authenticated Reflected Cross-Site Scripting vulnerabilities. The 'check_out_date' parameter of the reservation.php resource is copied into the HTML document as plain text between tags. Any input is echoed unmodified in	https://www.kashipara.com/	A-KAS-HOTE-160124/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the application's response. **CVE ID : CVE-2023-49271**		
Product: job_portal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'cmbQual' parameter of the Employer/InsertJob.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49677**	N/A	A-KAS-JOB_-160124/333
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtDesc' parameter of the Employer/InsertJob.php resource does not validate the characters received	N/A	A-KAS-JOB_-160124/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and they are sent unfiltered to the database. **CVE ID : CVE-2023-49678**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtTitle' parameter of the Employer/InsertJob.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49679**	N/A	A-KAS-JOB_-160124/335
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtTotal' parameter of the Employer/InsertJob.php resource does not validate the characters received and they are sent	N/A	A-KAS-JOB_-160124/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unfiltered to the database. **CVE ID : CVE-2023-49680**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'cmbQual' parameter of the Employer/InsertWalkin.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49681**	N/A	A-KAS-JOB_-160124/337
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtDate' parameter of the Employer/InsertWalkin.php resource does not validate the characters received and they are sent	N/A	A-KAS-JOB_-160124/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unfiltered to the database. **CVE ID : CVE-2023-49682**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtDesc' parameter of the Employer/InsertWalkin.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49683**	N/A	A-KAS-JOB_-160124/339
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtTitle' parameter of the Employer/InsertWalkin.php resource does not validate the characters received and they are sent	N/A	A-KAS-JOB_-160124/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unfiltered to the database. **CVE ID : CVE-2023-49684**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtTime' parameter of the Employer/InsertWalkin.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49685**	N/A	A-KAS-JOB_-160124/341
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtTotal' parameter of the Employer/InsertWalkin.php resource does not validate the characters received and they are sent	N/A	A-KAS-JOB_-160124/342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unfiltered to the database. **CVE ID : CVE-2023-49686**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtPass' parameter of the login.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49687**	N/A	A-KAS-JOB_-160124/343
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txtUser' parameter of the login.php resource does not validate the characters received and they are sent unfiltered to the database.	N/A	A-KAS-JOB_-160124/344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49688		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'JobId' parameter of the Employer/DeleteJob.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-49689**	N/A	A-KAS-JOB_-160124/345
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2023	9.8	Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'WalkinId' parameter of the Employer/DeleteJob.php resource does not validate the characters received and they are sent unfiltered to the database.	N/A	A-KAS-JOB_-160124/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49690		
Product: student_information_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Student Information System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'id' parameter of the marks.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-5007**	N/A	A-KAS-STUD-160124/347
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Student Information System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'coursecode' parameter of the marks.php resource does not validate the characters received and they are sent unfiltered to the database.	N/A	A-KAS-STUD-160124/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5010		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Student Information System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'coursename' parameter of the marks.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-5011**	N/A	A-KAS-STUD-160124/349
Vendor: kitty_project					
Product: kitty					
Affected Version(s): * Up to (including) 0.76.1.13					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42,	A-KIT-KITT-160124/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh	https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: kodcloud					
Product: kodbox					
Affected Version(s): * Up to (excluding) 1.48.04					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2023	9.8	A vulnerability was found in kalcaddle kodbox up to 1.48. It has been declared as critical. Affected by this vulnerability is the function check of the file plugins/officeViewer/controller/libreOffice/index.class.php. The manipulation of the	https://github.com/kalcaddle/kodbox/commit/63a4d5708d210f119c24afd941d01a943e25334c	A-KOD-KODB-160124/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument soffice leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.48.04 is able to address this issue. The identifier of the patch is 63a4d5708d210f119c24afd941d01a943e25334c. It is recommended to upgrade the affected component. The identifier VDB-248209 was assigned to this vulnerability. **CVE ID : CVE-2023-6848**		
Server-Side Request Forgery (SSRF)	16-Dec-2023	9.8	A vulnerability was found in kalcaddle kodbox up to 1.48. It has been rated as critical. Affected by this issue is the function cover of the file plugins/fileThumb/app.php. The manipulation of the argument path leads to server-side request forgery. The attack may be launched remotely.	https://github.com/kalcaddle/kodbox/commit/63a4d5708d210f119c24afd941d01a943e25334c	A-KOD-KODB-160124/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. Upgrading to version 1.48.04 is able to address this issue. The patch is identified as 63a4d5708d210f119c24afd941d01a943e25334c. It is recommended to upgrade the affected component. VDB-248210 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-6849**		
Product: kodexplorer					
Affected Version(s): * Up to (excluding) 4.52.01					
Unrestricted Upload of File with Dangerous Type	16-Dec-2023	9.8	A vulnerability was found in kalcaddle KodExplorer up to 4.51.03. It has been declared as critical. This vulnerability affects unknown code of the file /index.php?pluginApp/to/yzOffice/getFile of the component API Endpoint Handler. The manipulation of the argument path/file leads to unrestricted upload. The attack can be initiated	https://github.com/kalcaddle/KodExplorer/commit/5cf233f7556b442100cf67b5e92d57ceabb126c6	A-KOD-KODE-160124/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.52.01 is able to address this issue. The patch is identified as 5cf233f7556b442100cf67b5e92d57ceabb126c6. It is recommended to upgrade the affected component. VDB-248218 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-6850**		
Improper Control of Generation of Code ('Code Injection')	16-Dec-2023	9.8	A vulnerability was found in kalcaddle KodExplorer up to 4.51.03. It has been rated as critical. This issue affects the function unzipList of the file plugins/zipView/app.php of the component ZIP Archive Handler. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading	https://github.com/kalcaddle/KodExplorer/commit/5cf233f7556b442100cf67b5e92d57ceabb126c6	A-KOD-KODE-160124/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to version 4.52.01 is able to address this issue. The patch is named 5cf233f7556b442100cf67b5e92d57ceabb126c6. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-248219. **CVE ID : CVE-2023-6851**		
Server-Side Request Forgery (SSRF)	16-Dec-2023	9.8	A vulnerability classified as critical has been found in kalcaddle KodExplorer up to 4.51.03. Affected is an unknown function of the file plugins/webodf/app.php. The manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.52.01 is able to address this issue. The name of the patch is 5cf233f7556b442100cf67b5e92d57ce	https://github.com/kalcaddle/KodExplorer/commit/5cf233f7556b442100cf67b5e92d57ceabb126c6	A-KOD-KODE-160124/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			abb126c6. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248220. **CVE ID : CVE-2023-6852**		
Server-Side Request Forgery (SSRF)	16-Dec-2023	9.8	A vulnerability classified as critical was found in kalcaddle KodExplorer up to 4.51.03. Affected by this vulnerability is the function index of the file plugins/officeLive/app.php. The manipulation of the argument path leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.52.01 is able to address this issue. The identifier of the patch is 5cf233f7556b442100cf67b5e92d57ceabb126c6. It is recommended to upgrade the affected	https://github.com/kalcaddle/KodExplorer/commit/5cf233f7556b442100cf67b5e92d57ceabb126c6	A-KOD-KODE-160124/356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component. The identifier VDB-248221 was assigned to this vulnerability. **CVE ID : CVE-2023-6853**		
Affected Version(s): 4.51					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2023	6.1	Reflective Cross Site Scripting (XSS) vulnerability in KodeExplorer version 4.51, allows attackers to obtain sensitive information and escalate privileges via the APP_HOST parameter at config/i18n/en/main.php. **CVE ID : CVE-2023-49489**	N/A	A-KOD-KODE-160124/357
Vendor: lfprojects					
Product: mlflow					
Affected Version(s): * Up to (excluding) 2.9.2					
Server-Side Request Forgery (SSRF)	20-Dec-2023	9.8	A malicious user could use this issue to access internal HTTP(s) servers and in the worst case (ie: aws instance) it could be abuse to get a remote code execution on the victim machine. **CVE ID : CVE-2023-6974**	https://github.com/mlflow/mlflow/commit/8174250f83352a04c2d42079f414759060458555	A-LFP-MLFL-160124/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Path Traversal: '..filename'	20-Dec-2023	9.8	A malicious user could use this issue to get command execution on the vulnerable machine and get access to data & models information. **CVE ID : CVE-2023-6975**	https://github.com/mlflow/mlflow/commit/b9ab9ed77e1deda9697fe472fb1079fd428149ee	A-LFP-MLFL-160124/359
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Dec-2023	8.8	with only one user interaction(download a malicious config), attackers can gain full command execution on the victim system. **CVE ID : CVE-2023-6940**	https://github.com/mlflow/mlflow/commit/5139b1087d686fa52e2b087e09da66aff86297b1	A-LFP-MLFL-160124/360
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	This vulnerability is capable of writing arbitrary files into arbitrary locations on the remote filesystem in the context of the server process. **CVE ID : CVE-2023-6976**	https://github.com/mlflow/mlflow/commit/5044878da0c1851ccfdd5c0a867157ed9a502fbc	A-LFP-MLFL-160124/361
Path Traversal: '..filename'	18-Dec-2023	7.5	Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.9.2. **CVE ID : CVE-2023-6909**	https://huntr.com/bounties/11209efb-0f84-482f-add0-587ea6b7e850, https://github.com/mlflow/mlflow/commit/1da75dfcecd4d169e34809ade55748384e8af6c1	A-LFP-MLFL-160124/362

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.0.0 Up to (excluding) 2.9.2					
Path Traversal: '..filename'	20-Dec-2023	7.5	This vulnerability enables malicious users to read sensitive files on the server. **CVE ID : CVE-2023-6977**	https://github.com/mlflow/mlflow/commit/4bd7f27c810ba7487d53ed5ef1038fca0f8dc28c	A-LFP-MLFL-160124/363
Vendor: Libming					
Product: libming					
Affected Version(s): 0.4.8					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2023	9.8	Buffer Overflow vulnerability in libming version 0.4.8, allows attackers to execute arbitrary code and obtain sensitive information via parser.c component. **CVE ID : CVE-2023-50628**	https://github.com/libming/libming/pull/290	A-LIB-LIBM-160124/364
Vendor: Libssh					
Product: libssh					
Affected Version(s): * Up to (excluding) 0.10.6					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42,	A-LIB-LIBS-160124/365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh	https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Libssh2					
Product: libssh2					
Affected Version(s): * Up to (excluding) 1.11.10					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.c	A-LIB-LIBS-160124/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in	om/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Libtiff					
Product: libtiff					
Affected Version(s): -					
Out-of-bounds Write	18-Dec-2023	5.5	An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash. **CVE ID : CVE-2023-6228**	https://access.redhat.com/security/cve/CVE-2023-6228, https://bugzilla.redhat.com/show_bug.cgi?id=2240995	A-LIB-LIBT-160124/367
Vendor: lindeni					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: who_hit_the_page_-_hit_counter					
Affected Version(s): * Up to (including) 1.4.14.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Dec-2023	6.5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mahlamusa Who Hit The Page – Hit Counter allows SQL Injection.This issue affects Who Hit The Page – Hit Counter: from n/a through 1.4.14.3. **CVE ID : CVE-2023-47558**	N/A	A-LIN-WHO_-160124/368
Vendor: linkwhisper					
Product: link_whisper_free					
Affected Version(s): * Up to (excluding) 0.6.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Link Whisper Link Whisper Free.This issue affects Link Whisper Free: from n/a through 0.6.5. **CVE ID : CVE-2023-47852**	N/A	A-LIN-LINK-160124/369

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: linotp					
Product: linotp					
Affected Version(s): From (including) 3.0.0 Up to (including) 3.2.4					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	6.8	Defective request context handling in Self Service in LinOTP 3.x before 3.2.5 allows remote unauthenticated attackers to escalate privileges, thereby allowing them to act as and with the permissions of another user. Attackers must generate repeated API requests to trigger a race condition with concurrent user activity in the self-service portal. **CVE ID : CVE-2023-49706**	https://www.linotp.org/news.html, https://linotp.org/CVE-2023-49706.txt, https://linotp.org/security-update-linotp3-selfservice.html	A-LIN-LINO-160124/370
Product: virtual_appliance					
Affected Version(s): From (including) 3.0.0 Up to (including) 3.2.4					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	6.8	Defective request context handling in Self Service in LinOTP 3.x before 3.2.5 allows remote unauthenticated attackers to escalate privileges, thereby allowing them to act as and with the permissions of another user. Attackers must	https://www.linotp.org/news.html, https://linotp.org/CVE-2023-49706.txt, https://linotp.org/security-update-linotp3-selfservice.html	A-LIN-VIRT-160124/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			generate repeated API requests to trigger a race condition with concurrent user activity in the self-service portal. **CVE ID : CVE-2023-49706**		
Vendor: livechat					
Product: livechat					
Affected Version(s): * Up to (including) 4.5.15					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in LiveChat LiveChat – WP live chat plugin for WordPress.This issue affects LiveChat – WP live chat plugin for WordPress: from n/a through 4.5.15. **CVE ID : CVE-2023-49821**	N/A	A-LIV-LIVE-160124/372
Vendor: m-files					
Product: m-files_server					
Affected Version(s): * Up to (excluding) 23.12.13195.0					
N/A	20-Dec-2023	6.5	A vulnerable API method in M-Files Server before 23.12.13195.0 allows for uncontrolled resource consumption. Authenticated	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-6910	A-M-F-M-FI-160124/373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can exhaust server storage space to a point where the server can no longer serve requests. **CVE ID : CVE-2023-6910**		
Affected Version(s): * Up to (excluding) 23.12.13205.0					
Improper Restriction of Excessive Authentication Attempts	20-Dec-2023	9.8	Lack of protection against brute force attacks in M-Files Server before 23.12.13205.0 allows an attacker unlimited authentication attempts, potentially compromising targeted M-Files user accounts by guessing passwords. **CVE ID : CVE-2023-6912**	https://www.m-files.com/about/trust-center/security-advisories/cve-2023-6912/	A-M-F-M-FI-160124/374
Vendor: madebytribe					
Product: caddy					
Affected Version(s): * Up to (excluding) 1.9.8					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tribe Interactive Caddy – Smart Side Cart for WooCommerce.This issue affects Caddy – Smart Side Cart for	N/A	A-MAD-CADD-160124/375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WooCommerce: from n/a through 1.9.7. **CVE ID : CVE-2023-49854**		
Vendor: magazine3					
Product: core_web_vitals_\&_pagespeed_booster					
Affected Version(s): * Up to (including) 1.0.12					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2023	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Magazine3 Core Web Vitals & PageSpeed Booster.This issue affects Core Web Vitals & PageSpeed Booster: from n/a through 1.0.12. **CVE ID : CVE-2023-35883**	N/A	A-MAG-CORE-160124/376
Vendor: magiclogix					
Product: msync					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Magic Logix MSync.This issue	N/A	A-MAG-MSYN-160124/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects MSync: from n/a through 1.0.0. **CVE ID : CVE-2023-49166**		
Vendor: mainwp					
Product: mainwp_dashboard					
Affected Version(s): * Up to (excluding) 4.4.3.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	4.9	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MainWP MainWP Dashboard – WordPress Manager for Multiple Websites Maintenance.This issue affects MainWP Dashboard – WordPress Manager for Multiple Websites Maintenance: from n/a through 4.4.3.3. **CVE ID : CVE-2023-38519**	N/A	A-MAI-MAIN-160124/378
Vendor: marketingrapel					
Product: mkrapel_regiones_y_ciudades_de_chile_para_wc					
Affected Version(s): * Up to (including) 4.3.0					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Marketing Rapel MkRapel Regiones y Ciudades de Chile para WC.This issue affects MkRapel Regiones y Ciudades de Chile para WC: from n/a through 4.3.0. **CVE ID : CVE-2023-48781**	N/A	A-MAR-MKRA-160124/379
Vendor: masterslider					
Product: master_slider					
Affected Version(s): * Up to (including) 3.6.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Dec-2023	8.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Master slider Master Slider Pro allows SQL Injection.This issue affects Master Slider Pro: from n/a through 3.6.5. **CVE ID : CVE-2023-47506**	N/A	A-MAS-MAST-160124/380
Vendor: matez					
Product: jsch					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 0.2.15					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-MAT-JSCH-160124/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: maurice					
Product: vrm360					
Affected Version(s): * Up to (including) 1.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	18-Dec-2023	8.8	The Vrm 360 3D Model Viewer WordPress plugin through 1.2.1 is vulnerable to arbitrary file upload due to insufficient checks in a plugin shortcode. **CVE ID : CVE-2023-4311**	N/A	A-MAU-VRM3-160124/382
Vendor: mayurik					
Product: online_student_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2023	4.8	A vulnerability has been found in SourceCodester Online Student Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file edit-student-detail.php. The manipulation of the argument notmsg 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-248377 was	N/A	A-MAY-ONLI-160124/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-6945**		
Vendor: mayuri_k					
Product: best_courier_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Dec-2023	9.8	A vulnerability classified as critical has been found in SourceCodester Best Courier Management System 1.0. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248256. **CVE ID : CVE-2023-6898**	N/A	A-MAY-BEST-160124/384
Vendor: Mediawiki					
Product: mediawiki					
Affected Version(s): * Up to (excluding) 1.35.14					
Improper Neutralization of Input During Web Page Generation	22-Dec-2023	6.1	An issue was discovered in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. In	https://phabricator.wikimedia.org/T347726	A-MED-MEDI-160124/385

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			includes/logging/RightsLogFormatter.php, group-*-member messages can result in XSS on Special:log/rights. **CVE ID : CVE-2023-51704**		
Affected Version(s): From (including) 1.36.0 Up to (excluding) 1.39.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	6.1	An issue was discovered in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. In includes/logging/RightsLogFormatter.php, group-*-member messages can result in XSS on Special:log/rights. **CVE ID : CVE-2023-51704**	https://phabricator.wikimedia.org/T347726	A-MED-MEDI-160124/386
Affected Version(s): From (including) 1.40.0 Up to (excluding) 1.40.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	6.1	An issue was discovered in MediaWiki before 1.35.14, 1.36.x through 1.39.x before 1.39.6, and 1.40.x before 1.40.2. In includes/logging/RightsLogFormatter.php, group-*-member messages can result in XSS on Special:log/rights.	https://phabricator.wikimedia.org/T347726	A-MED-MEDI-160124/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51704		
Vendor: meowapps					
Product: media_file_renamer_-_auto_\&_manual_rename					
Affected Version(s): * Up to (including) 5.6.9					
N/A	19-Dec-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jordy Meow Media File Renamer: Rename Files (Manual, Auto & AI).This issue affects Media File Renamer: Rename Files (Manual, Auto & AI): from n/a through 5.6.9. **CVE ID : CVE-2023-44991**	N/A	A-MEO-MEDI-160124/388
Product: photo_engine					
Affected Version(s): * Up to (excluding) 6.2.6					
Authorization Bypass Through User-Controlled Key	20-Dec-2023	5.4	Authorization Bypass Through User-Controlled Key vulnerability in Jordy Meow Photo Engine (Media Organizer & Lightroom).This issue affects Photo Engine (Media Organizer & Lightroom): from n/a through 6.2.5.	N/A	A-MEO-PHOT-160124/389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-38513		
Vendor: Microsoft					
Product: powershell					
Affected Version(s): * Up to (including) 11.1.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-MIC-POWE-160124/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48795		
Vendor: mondula					
Product: multi_step_form					
Affected Version(s): * Up to (including) 1.7.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mondula GmbH Multi Step Form allows Stored XSS.This issue affects Multi Step Form: from n/a through 1.7.13. **CVE ID : CVE-2023-50832**	N/A	A-MON-MULT-160124/391
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 121.0					
Out-of-bounds Write	19-Dec-2023	8.8	The WebGL `DrawElementsInstanced` method was susceptible to a heap buffer overflow when used on systems with the Mesa VM driver. This issue could allow an attacker to perform remote code execution and sandbox escape.	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6856**		
Out-of-bounds Write	19-Dec-2023	8.8	Firefox was susceptible to a heap buffer overflow in `nsTextFragment` due to insufficient OOM handling. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6858**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/393
Use After Free	19-Dec-2023	8.8	A use-after-free condition affected TLS socket creation when under memory pressure. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6859**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/394
Out-of-bounds Write	19-Dec-2023	8.8	The `nsWindow::PickerOpen(void)` method was susceptible to a heap buffer	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/secur	A-MOZ-FIRE-160124/395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow when running in headless mode. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6861**	ity/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	
N/A	19-Dec-2023	8.8	The `ShutdownObserver()` was susceptible to potentially undefined behavior due to its reliance on a dynamic type that lacked a virtual destructor. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6863**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/396
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code.	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6864**		
Improper Handling of Exceptional Conditions	19-Dec-2023	8.8	TypedArrays can be fallible and lacked proper exception handling. This could lead to abuse in other APIs which expect TypedArrays to always succeed. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6866**	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/398
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6873**	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/399
N/A	19-Dec-2023	6.5	The `VideoBridge` allowed any content process to	https://www.mozilla.org/security/advisories/	A-MOZ-FIRE-160124/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use textures produced by remote decoders. This could be abused to escape the sandbox. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6860**	mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	
N/A	19-Dec-2023	6.5	`EncryptingOutputStream` was susceptible to exposing uninitialized data. This issue could only be abused in order to write data to a local disk which may have implications for private browsing mode. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121. **CVE ID : CVE-2023-6865**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/401
N/A	19-Dec-2023	6.5	A `&lt;dialog>` element could have been manipulated to paint content outside of a sandboxed iframe. This could allow untrusted content to display under the guise of trusted	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6869**		
N/A	19-Dec-2023	6.5	Browser tab titles were being leaked by GNOME to system logs. This could potentially expose the browsing habits of users running in a private tab. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6872**	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/403
Improper Restriction of Rendered UI Layers or Frames	19-Dec-2023	6.1	The timing of a button click causing a popup to disappear was approximately the same length as the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121.	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6867		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	5.3	When resolving a symlink, a race may occur where the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/405
Observable Discrepancy	19-Dec-2023	4.3	Multiple NSS NIST curves were susceptible to a side-channel attack known as "Minerva". This attack could potentially allow an attacker to recover the private key. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6135**	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/406
N/A	19-Dec-2023	4.3	In some instances, the user-agent	https://www.mozilla.org/secur	A-MOZ-FIRE-160124/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would allow push requests which lacked a valid VAPID even though the push manager subscription defined one. This could allow empty messages to be sent from unauthorized parties. *This bug only affects Firefox on Android.* This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6868**	ity/advisories/ mfsa2023-56/	
N/A	19-Dec-2023	4.3	Applications which spawn a Toast notification in a background thread may have obscured fullscreen notifications displayed by Firefox. *This issue only affects Android versions of Firefox and Firefox Focus.* This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6870**	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/408
N/A	19-Dec-2023	4.3	Under certain conditions, Firefox did not display a warning when a	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user attempted to navigate to a new protocol handler. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6871**		
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 115.6					
Out-of-bounds Write	19-Dec-2023	8.8	The WebGL `DrawElementsInstanced` method was susceptible to a heap buffer overflow when used on systems with the Mesa VM driver. This issue could allow an attacker to perform remote code execution and sandbox escape. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6856**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/410
Out-of-bounds Write	19-Dec-2023	8.8	Firefox was susceptible to a heap buffer overflow in `nsTextFragment` due to insufficient OOM handling. This vulnerability affects Firefox ESR < 115.6,	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/secur	A-MOZ-FIRE-160124/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6858**	ity/advisories/mfsa2023-56/	
Use After Free	19-Dec-2023	8.8	A use-after-free condition affected TLS socket creation when under memory pressure. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6859**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/412
Out-of-bounds Write	19-Dec-2023	8.8	The `nsWindow::PickerOpen(void)` method was susceptible to a heap buffer overflow when running in headless mode. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6861**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/413
Use After Free	19-Dec-2023	8.8	A use-after-free was identified in the `nsDNSService::Init`. This issue appears to manifest rarely	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/secur	A-MOZ-FIRE-160124/414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during start-up. This vulnerability affects Firefox ESR < 115.6 and Thunderbird < 115.6. **CVE ID : CVE-2023-6862**	ity/advisories/mfsa2023-55/	
N/A	19-Dec-2023	8.8	The `ShutdownObserver()` was susceptible to potentially undefined behavior due to its reliance on a dynamic type that lacked a virtual destructor. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6863**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/415
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 115.6,	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6864**		
N/A	19-Dec-2023	6.5	The `VideoBridge` allowed any content process to use textures produced by remote decoders. This could be abused to escape the sandbox. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6860**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/417
N/A	19-Dec-2023	6.5	`EncryptingOutputStream` was susceptible to exposing uninitialized data. This issue could only be abused in order to write data to a local disk which may have implications for private browsing mode. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121. **CVE ID : CVE-2023-6865**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	19-Dec-2023	6.1	The timing of a button click causing a popup to disappear was approximately the same length as the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121. **CVE ID : CVE-2023-6867**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/419
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	5.3	When resolving a symlink, a race may occur where the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird <	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**		
Product: firefox_focus					
Affected Version(s): -					
N/A	19-Dec-2023	4.3	Applications which spawn a Toast notification in a background thread may have obscured fullscreen notifications displayed by Firefox. *This issue only affects Android versions of Firefox and Firefox Focus.* This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6870**	https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-FIRE-160124/421
Product: thunderbird					
Affected Version(s): * Up to (excluding) 115.6					
Out-of-bounds Write	19-Dec-2023	8.8	The WebGL `DrawElementsInstanced` method was susceptible to a heap buffer overflow when used on systems with the Mesa VM driver. This issue could allow an attacker to perform remote code execution and sandbox escape. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-THUN-160124/422

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6856**		
Out-of-bounds Write	19-Dec-2023	8.8	Firefox was susceptible to a heap buffer overflow in `nsTextFragment` due to insufficient OOM handling. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6858**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-THUN-160124/423
Use After Free	19-Dec-2023	8.8	A use-after-free condition affected TLS socket creation when under memory pressure. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6859**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-THUN-160124/424
Out-of-bounds Write	19-Dec-2023	8.8	The `nsWindow::PickerOpen(void)` method was susceptible to a heap buffer overflow when	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/	A-MOZ-THUN-160124/425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			running in headless mode. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6861**	mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	
Use After Free	19-Dec-2023	8.8	A use-after-free was identified in the `nsDNSService::Init`. This issue appears to manifest rarely during start-up. This vulnerability affects Firefox ESR < 115.6 and Thunderbird < 115.6. **CVE ID : CVE-2023-6862**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/	A-MOZ-THUN-160124/426
N/A	19-Dec-2023	8.8	The `ShutdownObserver()` was susceptible to potentially undefined behavior due to its reliance on a dynamic type that lacked a virtual destructor. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-THUN-160124/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6863		
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6864**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-THUN-160124/428
N/A	19-Dec-2023	6.5	The `VideoBridge` allowed any content process to use textures produced by remote decoders. This could be abused to escape the sandbox. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6860**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-THUN-160124/429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	5.3	When resolving a symlink, a race may occur where the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	A-MOZ-THUN-160124/430
N/A	19-Dec-2023	4.3	The signature of a digitally signed S/MIME email message may optionally specify the signature creation date and time. If present, Thunderbird did not compare the signature creation date with the message date and time, and displayed a valid signature despite a date or time mismatch. This could be used to give recipients the impression that a message was sent	https://www.mozilla.org/security/advisories/mfsa2023-55/	A-MOZ-THUN-160124/431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			at a different date or time. This vulnerability affects Thunderbird < 115.6. **CVE ID : CVE-2023-50761**		
N/A	19-Dec-2023	4.3	When processing a PGP/MIME payload that contains digitally signed text, the first paragraph of the text was never shown to the user. This is because the text was interpreted as a MIME message and the first paragraph was always treated as an email header section. A digitally signed text from a different context, such as a signed GIT commit, could be used to spoof an email message. This vulnerability affects Thunderbird < 115.6. **CVE ID : CVE-2023-50762**	https://www.mozilla.org/security/advisories/mfsa2023-55/	A-MOZ-THUN-160124/432
Vendor: mr-corner					
Product: amazing_little_poll					
Affected Version(s): 1.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Dec-2023	9.8	Authentication bypass vulnerability in Amazing Little Poll affecting versions 1.3 and 1.4. This vulnerability could allow an unauthenticated user to access the admin panel without providing any credentials by simply accessing the "lp_admin.php?adminstep=" parameter. **CVE ID : CVE-2023-6768**	N/A	A-MR--AMAZ-160124/433
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	4.6	Stored XSS vulnerability in Amazing Little Poll, affecting versions 1.3 and 1.4. This vulnerability allows a remote attacker to store a malicious JavaScript payload in the "lp_admin.php" file in the "question" and "item" parameters. This vulnerability could lead to malicious JavaScript execution while the page is loading. **CVE ID : CVE-2023-6769**	N/A	A-MR--AMAZ-160124/434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.4					
Improper Authentication	20-Dec-2023	9.8	Authentication bypass vulnerability in Amazing Little Poll affecting versions 1.3 and 1.4. This vulnerability could allow an unauthenticated user to access the admin panel without providing any credentials by simply accessing the "lp_admin.php?adminstep=" parameter. **CVE ID : CVE-2023-6768**	N/A	A-MR--AMAZ-160124/435
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	4.6	Stored XSS vulnerability in Amazing Little Poll, affecting versions 1.3 and 1.4. This vulnerability allows a remote attacker to store a malicious JavaScript payload in the "lp_admin.php" file in the "question" and "item" parameters. This vulnerability could lead to malicious JavaScript execution while the page is loading.	N/A	A-MR--AMAZ-160124/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6769		
Vendor: mtrv					
Product: teachpress					
Affected Version(s): * Up to (including) 9.0.5					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Michael Winkler teachPress.This issue affects teachPress: from n/a through 9.0.5. **CVE ID : CVE-2023-49163**	N/A	A-MTR-TEAC-160124/437
Vendor: multivendorx					
Product: product_catalog_mode_for_woocommerce					
Affected Version(s): * Up to (excluding) 5.0.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	6.1	The Product Catalog Mode For WooCommerce WordPress plugin before 5.0.3 does not properly authorize settings updates or escape settings values, leading to stored XSS by unauthenticated users. **CVE ID : CVE-2023-5348**	N/A	A-MUL-PROD-160124/438
Vendor: net-ssh					
Product: net-ssh					
Affected Version(s): 7.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-NET-NET--160124/439

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		

Vendor: netentsec

Product: application_security_gateway

Affected Version(s): 6.3.1

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Dec-2023	9.8	A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3.1. This affects an unknown part of the file /admin/singlelogin.php?submit=1. The manipulation of the argument loginId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248265 was assigned to this vulnerability. **CVE ID : CVE-2023-6903**	N/A	A-NET-APPL-160124/440
Vendor: Netgate					
Product: pfsense_ce					
Affected Version(s): * Up to (including) 2.7.2					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.	A-NET-PFSE-160124/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through	xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: pfsense_plus					
Affected Version(s): * Up to (including) 23.09.1					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/cry	A-NET-PFSE-160124/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP,	pto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Netsarang					
Product: xshell_7					
Affected Version(s): * Up to (excluding) build__0144					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d	A-NET-XSHE-160124/443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80,	2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Nextcloud					
Product: nextcloud					
Affected Version(s): * Up to (excluding) 4.9.2					
Improper Authentication	22-Dec-2023	4.3	The Nextcloud iOS Files app allows users of iOS to interact with Nextcloud, a self-hosted productivity platform. Prior to version 4.9.2, the application can be used without providing the 4 digit PIN code. Nextcloud iOS Files app should be upgraded to 4.9.2 to receive the	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-j8g7-88vv-rggv, https://github.com/nextcloud/ios/pull/2665	A-NEX-NEXT-160124/444

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			patch. No known workarounds are available. **CVE ID : CVE-2023-49790**		
Vendor: NOS					
Product: nos_client					
Affected Version(s): 0.6.6					
N/A	21-Dec-2023	9.8	An issue was discovered in nos client version 0.6.6, allows remote attackers to escalate privileges via getRPCEndpoint.js. **CVE ID : CVE-2023-50477**	N/A	A-NOS-NOS_-160124/445
Vendor: nxfilter					
Product: nxfilter					
Affected Version(s): 4.3.2.5					
Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	18-Dec-2023	9.8	A vulnerability, which was classified as problematic, has been found in Jahastech NxFilter 4.3.2.5. This issue affects some unknown processing of the file user,adap.jsp?actionFlag=test&id=1 of the component Bind Request Handler. The manipulation leads to ldap injection. The attack may be initiated remotely.	N/A	A-NXF-NXFI-160124/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The associated identifier of this vulnerability is VDB-248267. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6905**		
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	A vulnerability classified as problematic was found in Jahastech NxFilter 4.3.2.5. This vulnerability affects unknown code of the file /config,admin.jsp. The manipulation of the argument admin_name leads to cross-site request forgery. The attack can be initiated remotely. VDB-248266 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-2023-6904**	N/A	A-NXF-NXFI-160124/447
Vendor: oceanwp					
Product: ocean_extra					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.2.3					
Cross-Site Request Forgery (CSRF)	19-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in OceanWP Ocean Extra.This issue affects Ocean Extra: from n/a through 2.2.2. **CVE ID : CVE-2023-49164**	N/A	A-OCE-OCEA-160124/448
Vendor: olivethemes					
Product: olive_one_click_demo_import					
Affected Version(s): * Up to (including) 1.1.1					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	7.2	Unrestricted Upload of File with Dangerous Type vulnerability in Olive Themes Olive One Click Demo Import.This issue affects Olive One Click Demo Import: from n/a through 1.1.1. **CVE ID : CVE-2023-29102**	N/A	A-OLI-OLIV-160124/449
Vendor: Openbsd					
Product: openssh					
Affected Version(s): * Up to (excluding) 9.6					
Improper Neutralization of Special Elements	18-Dec-2023	9.8	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host	https://github.com/openssh/openssh-portable/commit/7ef3787c84b	A-OPE-OPEN-160124/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name. **CVE ID : CVE-2023-51385**	6b524501211b11a26c742f829af1a	
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-OPE-OPEN-160124/451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
N/A	18-Dec-2023	5.5	In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. **CVE ID : CVE-2023-51384**	https://github.com/openssh/openssh-portable/commit/881d9c6af9da4257c69c327c4e2f1508b2fa754b	A-OPE-OPEN-160124/452
Vendor: openimageio					
Product: openimageio					
Affected Version(s): 2.4.11					
Out-of-bounds Write	18-Dec-2023	7.5	A vulnerability was found in OpenImageIO, where a heap buffer overflow exists in the src/gif.imageio/gifi	N/A	A-OPE-OPEN-160124/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nput.cpp file. This flaw allows a remote attacker to pass a specially crafted file to the application, which triggers a heap-based buffer overflow and could cause a crash, leading to a denial of service. **CVE ID : CVE-2023-3430**		
Vendor: oretnom23					
Product: simple_image_stack_website					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2023	6.1	A vulnerability was found in SourceCodester Simple Image Stack Website 1.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument search with the input sy2ap%22%3e%3cscript%3ealert(1)%3c%2fscript%3etkxh1 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	N/A	A-ORE-SIMP-160124/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			identifier of this vulnerability is VDB-248255. **CVE ID : CVE-2023-6896**		
Product: simple_student_attendance_system					
Affected Version(s): 1.0					
Path Traversal: '../filedir'	22-Dec-2023	9.8	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument page leads to path traversal: '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248749 was assigned to this vulnerability. **CVE ID : CVE-2023-7058**	N/A	A-ORE-SIMP-160124/455
Vendor: oryx-embedded					
Product: cyclone_ssh					
Affected Version(s): * Up to (excluding) 2.3.4					
Improper Validation of Integrity	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH	https://github.com/openssh/openssh-	A-ORY-CYCL-160124/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Check Value		🟨	extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC	portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: pagevisitcounter					
Product: advanced_page_visit_counter					
Affected Version(s): * Up to (including) 6.4.2					
Improper Neutralization of Special	20-Dec-2023	8.8	Improper Neutralization of Special Elements used in an SQL	N/A	A-PAG-ADVA-160124/457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Command ('SQL Injection') vulnerability in Page Visit Counter Advanced Page Visit Counter – Most Wanted Analytics Plugin for WordPress.This issue affects Advanced Page Visit Counter – Most Wanted Analytics Plugin for WordPress: from n/a through 6.4.2. **CVE ID : CVE-2023-28788**		
Vendor: palscode					
Product: multi_currency_for_woocommerce					
Affected Version(s): * Up to (including) 1.5.5					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Palscode Multi Currency For WooCommerce.This issue affects Multi Currency For WooCommerce: from n/a through 1.5.5. **CVE ID : CVE-2023-49840**	N/A	A-PAL-MULT-160124/458
Vendor: panic					
Product: nova					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 11.8					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-PAN-NOVA-160124/459

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: transmit_5					
Affected Version(s): * Up to (excluding) 5.10.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-PAN-TRAN-160124/460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: paramiko					
Product: paramiko					
Affected Version(s): * Up to (excluding) 3.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-PAR-PARA-160124/461

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: parcelpro					
Product: parcel_pro					
Affected Version(s): * Up to (including) 1.6.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2023	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Parcel Pro.This issue affects Parcel Pro: from n/a through 1.6.11. **CVE ID : CVE-2023-46624**	N/A	A-PAR-PARC-160124/462
Vendor: paxton-access					
Product: net2					
Affected Version(s): 6.07					
Use of Hard-coded Credentials	19-Dec-2023	9.8	When installing the Net2 software a root certificate is installed into the trusted store. A potential hacker could access the installer batch file or reverse engineer the source code to gain access to the root certificate password. Using the root certificate and password they could then create their own certificates to emulate another site. Then by establishing a proxy service to emulate the site they could monitor traffic passed between the end user and the site	N/A	A-PAX-NET2-160124/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowing access to the data content. **CVE ID : CVE-2023-43870**		
Affected Version(s): From (including) 6.02 Up to (excluding) 6.07					
Use of Hard-coded Credentials	19-Dec-2023	9.8	When installing the Net2 software a root certificate is installed into the trusted store. A potential hacker could access the installer batch file or reverse engineer the source code to gain access to the root certificate password. Using the root certificate and password they could then create their own certificates to emulate another site. Then by establishing a proxy service to emulate the site they could monitor traffic passed between the end user and the site allowing access to the data content. **CVE ID : CVE-2023-43870**	N/A	A-PAX-NET2-160124/464
Vendor: paytr					
Product: paytr_taksit_tablosu_-_woocommerce					
Affected Version(s): * Up to (including) 1.3.1					
Cross-Site Request	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF)	N/A	A-PAY-PAYT-160124/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			vulnerability in PayTR Ödeme ve Elektronik Para Kurulu?u A.?. PayTR Taksit Tablosu – WooCommerce.This issue affects PayTR Taksit Tablosu – WooCommerce: from n/a through 1.3.1. **CVE ID : CVE-2023-49853**		
Vendor: peazip					
Product: peazip					
Affected Version(s): 9.4.0					
Uncontrolled Search Path Element	17-Dec-2023	7.8	A vulnerability has been found in PeaZip 9.4.0 and classified as problematic. Affected by this vulnerability is an unknown functionality in the library dragdropfilesdll.dll of the component Library Handler. The manipulation leads to uncontrolled search path. An attack has to be approached locally. Upgrading to version 9.6.0 is able to address this	N/A	A-PEA-PEAZ-160124/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-248251. NOTE: Vendor was contacted early, confirmed the existence of the flaw and immediately worked on a patched release. **CVE ID : CVE-2023-6891**		
Vendor: pencidesign					
Product: soledad					
Affected Version(s): * Up to (excluding) 8.4.2					
Deserialization of Untrusted Data	21-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in PenciDesign Soledad – Multipurpose, Newspaper, Blog & WooCommerce WordPress Theme.This issue affects Soledad – Multipurpose, Newspaper, Blog & WooCommerce WordPress Theme: from n/a through 8.4.1.	N/A	A-PEN-SOLE-160124/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49826		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	8.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in PenciDesign Soledad – Multipurpose, Newspaper, Blog & WooCommerce WordPress Theme.This issue affects Soledad – Multipurpose, Newspaper, Blog & WooCommerce WordPress Theme: from n/a through 8.4.1. **CVE ID : CVE-2023-49825**	N/A	A-PEN-SOLE-160124/468
Vendor: Perl					
Product: Perl					
Affected Version(s): 5.34.0					
Out-of-bounds Write	18-Dec-2023	7.8	A vulnerability was found in perl. This issue occurs when a crafted regular expression is compiled by perl, which can allow an attacker controlled byte buffer overflow in a heap allocated buffer.	https://access.redhat.com/security/cve/CVE-2023-47038, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1056746	A-PER-PERL-160124/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47038		
Vendor: Pexip					
Product: pexip_infinity					
Affected Version(s): * Up to (excluding) 31.2					
Improper Input Validation	25-Dec-2023	7.5	Pexip Infinity before 31.2 has Improper Input Validation for signalling, allowing remote attackers to trigger an abort. **CVE ID : CVE-2023-31289**	https://docs.pexip.com/admin/security_bulletins.htm	A-PEX-PEXI-160124/470
Improper Input Validation	25-Dec-2023	7.5	Pexip Infinity before 31.2 has Improper Input Validation for RTCP, allowing remote attackers to trigger an abort. **CVE ID : CVE-2023-31455**	https://docs.pexip.com/admin/security_bulletins.htm	A-PEX-PEXI-160124/471
Affected Version(s): * Up to (excluding) 32.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Dec-2023	6.1	Pexip Infinity before 32 allows Webapp1 XSS via preconfigured links. **CVE ID : CVE-2023-37225**	https://docs.pexip.com/admin/security_bulletins.htm	A-PEX-PEXI-160124/472
Product: virtual_meeting_rooms					
Affected Version(s): * Up to (excluding) 3.0					
Use of Hard-coded Credentials	25-Dec-2023	5.3	In Pexip VMR self-service portal before 3, the same SSH host key is used across	https://docs.pexip.com/admin/security_bulletins.htm	A-PEX-VIRT-160124/473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different customers' installations, which allows authentication bypass. **CVE ID : CVE-2023-40236**		
Vendor: phpbits					
Product: genesis_simple_love					
Affected Version(s): * Up to (including) 2.0					
Deserialization of Untrusted Data	20-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in Phpbits Creative Studio Genesis Simple Love.This issue affects Genesis Simple Love: from n/a through 2.0. **CVE ID : CVE-2023-49772**	N/A	A-PHP-GENE-160124/474
Vendor: phpgurukul					
Product: nipah_virus_testing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Dec-2023	9.8	A vulnerability, which was classified as critical, has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This issue affects some unknown processing of the	N/A	A-PHP-NIPA-160124/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file bwdates-report-result.php. The manipulation of the argument fromdate 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-248951. **CVE ID : CVE-2023-7099**		
Product: online_notes_sharing_system					
Affected Version(s): 1.0					
Weak Password Requirements	22-Dec-2023	8.8	A vulnerability was found in PHPGurukul Online Notes Sharing System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /user/signup.php. The manipulation leads to weak password requirements. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The	N/A	A-PHP-ONLI-160124/476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248740. **CVE ID : CVE-2023-7053**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	A vulnerability has been found in PHPGurukul Online Notes Sharing System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file user/profile.php. The manipulation of the argument name/email 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-248737 was assigned to this vulnerability. **CVE ID : CVE-2023-7050**	N/A	A-PHP-ONLI-160124/477
Improper Neutralization of Input During	22-Dec-2023	5.4	A vulnerability was found in PHPGurukul Online Notes Sharing System 1.0. It has	N/A	A-PHP-ONLI-160124/478

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			been rated as problematic. This issue affects some unknown processing of the file /user/add-notes.php. The manipulation leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248741 was assigned to this vulnerability. **CVE ID : CVE-2023-7054**		
Incorrect Permission Assignment for Critical Resource	22-Dec-2023	5.4	A vulnerability classified as problematic has been found in PHPGurukul Online Notes Sharing System 1.0. Affected is an unknown function of the file /user/profile.php of the component Contact Information Handler. The manipulation of the argument mobilenumber leads to improper access controls. It is possible to launch the attack	N/A	A-PHP-ONLI-160124/479

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remotely. The exploit has been disclosed to the public and may be used. VDB-248742 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-7055**		
Cross-Site Request Forgery (CSRF)	21-Dec-2023	4.3	A vulnerability was found in PHPGurukul Online Notes Sharing System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /user/manage-notes.php of the component Notes Handler. The manipulation of the argument delid leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-248738 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-7051**	N/A	A-PHP-ONLI-160124/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	22-Dec-2023	4.3	A vulnerability was found in PHPGurukul Online Notes Sharing System 1.0. It has been classified as problematic. This affects an unknown part of the file /user/profile.php. The manipulation of the argument name leads to cross-site request forgery. 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-248739. **CVE ID : CVE-2023-7052**	N/A	A-PHP-ONLI-160124/481
Product: restaurant_table_booking_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-Dec-2023	9.8	A vulnerability, which was classified as critical, was found in PHPGurukul Restaurant Table Booking System 1.0. Affected is an unknown function of the file /admin/bwdates-report-details.php. The manipulation	N/A	A-PHP-REST-160124/482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument fdate 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-248952. **CVE ID : CVE-2023-7100**		
Product: student_result_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Student Result Management System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'class_name' parameter of the add_students.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48718**	N/A	A-PHP-STUD-160124/483
Improper Neutralization of Special	21-Dec-2023	9.8	Student Result Management System v1.0 is vulnerable to	N/A	A-PHP-STUD-160124/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			multiple Unauthenticated SQL Injection vulnerabilities. The 'roll_no' parameter of the add_students.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48719**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Student Result Management System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'password' parameter of the login.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48720**	N/A	A-PHP-STUD-160124/485
Improper Neutralization of	21-Dec-2023	9.8	Student Result Management System v1.0 is	N/A	A-PHP-STUD-160124/486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an SQL Command ('SQL Injection')			vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'class_name' parameter of the add_results.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48722**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Student Result Management System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'rno' parameter of the add_results.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48723**	N/A	A-PHP-STUD-160124/487
Vendor: Phpmyfaq					
Product: phpmyfaq					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.1.17					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.17. **CVE ID : CVE-2023-6889**	https://huntr.com/bounties/52897778-fad7-4169-bf04-a68a0646df0c, https://github.com/thorsten/phpmyfaq/commit/1037a8f012e0d9ec4bf4c8107972f6695e381392	A-PHP-PHPM-160124/488
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.17. **CVE ID : CVE-2023-6890**	https://huntr.com/bounties/2cf11678-8793-4fa1-b21a-f135564a105d, https://github.com/thorsten/phpmyfaq/commit/97d90ebbe11ebc6081bf49a2ba4b60f227cd1b43	A-PHP-PHPM-160124/489
Vendor: phz76					
Product: rtspserver					
Affected Version(s): 1.0.0					
Out-of-bounds Write	17-Dec-2023	9.8	A vulnerability classified as critical was found in PHZ76 RtspServer 1.0.0. This vulnerability affects the function ParseRequestLine of the file RtspMesaage.cpp. The manipulation leads to stack-based buffer overflow. The	N/A	A-PHZ-RTSP-160124/490

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248248. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6888**		
Vendor: pixelyoursite					
Product: product_catalog_feed					
Affected Version(s): * Up to (excluding) 2.2.0					
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in PixelYourSite Product Catalog Feed by PixelYourSite.This issue affects Product Catalog Feed by PixelYourSite: from n/a through 2.1.1. **CVE ID : CVE-2023-49824**	N/A	A-PIX-PROD-160124/491
Vendor: plugin-planet					
Product: user_submitted_posts					
Affected Version(s): * Up to (including) 20230902					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in Jeff Starr User Submitted Posts – Enable Users to Submit Posts from the Front End.This issue affects User Submitted Posts – Enable Users to Submit Posts from the Front End: from n/a through 20230902. **CVE ID : CVE-2023-45603**	N/A	A-PLU-USER-160124/492
Vendor: pluginus					
Product: fox_-_currency_switcher_professional_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.4.1.5					
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 FOX – Currency Switcher Professional for WooCommerce.This issue affects FOX – Currency Switcher Professional for WooCommerce: from n/a through 1.4.1.4.	N/A	A-PLU-FOX_-160124/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49834		
Product: husky_-_products_filter_professional_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.3.4.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in realmag777 HUSKY – Products Filter for WooCommerce Professional.This issue affects HUSKY – Products Filter for WooCommerce Professional: from n/a through 1.3.4.2. **CVE ID : CVE-2023-40010**	N/A	A-PLU-HUSK-160124/494
Vendor: portotheme					
Product: functionality					
Affected Version(s): * Up to (excluding) 2.12.1					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Porto Theme Porto Theme - Functionality.This issue affects Porto Theme -	N/A	A-POR-FUNC-160124/495

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Functionality: from n/a before 2.12.1. **CVE ID : CVE-2023-48738**		
Vendor: premio					
Product: folders					
Affected Version(s): * Up to (including) 2.9.2					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	7.2	Unrestricted Upload of File with Dangerous Type vulnerability in Premio Folders – Unlimited Folders to Organize Media Library Folder, Pages, Posts, File Manager.This issue affects Folders – Unlimited Folders to Organize Media Library Folder, Pages, Posts, File Manager: from n/a through 2.9.2. **CVE ID : CVE-2023-40204**	N/A	A-PRE-FOLD-160124/496
Vendor: Proftpd					
Product: proftpd					
Affected Version(s): * Up to (including) 1.3.8b					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other	https://github.com/openssh/openssh-portable/commits/master, https://github.c	A-PRO-PROF-160124/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms.	om/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Progress					
Product: sitefinity					
Affected Version(s): From (including) 14.1 Up to (excluding) 14.1.7828					
N/A	20-Dec-2023	4.3	A malicious user could potentially use the Sitefinity system for the distribution of phishing emails.	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-	A-PRO-SITE-160124/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6784	Vulnerability-CVE-2023-6784-December-2023	
Affected Version(s): From (including) 14.2 Up to (excluding) 14.2.7932					
N/A	20-Dec-2023	4.3	A malicious user could potentially use the Sitefinity system for the distribution of phishing emails. **CVE ID : CVE-2023-6784**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerability-CVE-2023-6784-December-2023	A-PRO-SITE-160124/499
Affected Version(s): From (including) 14.3 Up to (excluding) 14.3.8029					
N/A	20-Dec-2023	4.3	A malicious user could potentially use the Sitefinity system for the distribution of phishing emails. **CVE ID : CVE-2023-6784**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerability-CVE-2023-6784-December-2023	A-PRO-SITE-160124/500
Affected Version(s): From (including) 14.4 Up to (excluding) 14.4.8133					
N/A	20-Dec-2023	4.3	A malicious user could potentially use the Sitefinity system for the distribution of phishing emails.	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerability-CVE-2023-	A-PRO-SITE-160124/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6784	6784-December-2023	
Affected Version(s): From (including) 15.0 Up to (excluding) 15.0.8223					
N/A	20-Dec-2023	4.3	A malicious user could potentially use the Sitefinity system for the distribution of phishing emails. **CVE ID : CVE-2023-6784**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerability-CVE-2023-6784-December-2023	A-PRO-SITE-160124/502
Affected Version(s): From (including) 4.0 Up to (excluding) 13.3.7648					
N/A	20-Dec-2023	4.3	A malicious user could potentially use the Sitefinity system for the distribution of phishing emails. **CVE ID : CVE-2023-6784**	https://community.progress.com/s/article/Sitefinity-Security-Advisory-for-Addressing-Security-Vulnerability-CVE-2023-6784-December-2023	A-PRO-SITE-160124/503
Vendor: projectworlds					
Product: leave_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	21-Dec-2023	8.8	Leave Management System Project v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'setearnleave'	N/A	A-PRO-LEAV-160124/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			parameter of the admin/setleaves.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-44481**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Leave Management System Project v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'setsickleave' parameter of the admin/setleaves.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-44482**	N/A	A-PRO-LEAV-160124/505
Product: online_examination_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection	N/A	A-PRO-ONLI-160124/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			vulnerabilities. The 'ch' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45115**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'demail' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45116**	N/A	A-PRO-ONLI-160124/507
Improper Neutralization of Special Elements used in an SQL Command	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The	N/A	A-PRO-ONLI-160124/508

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			'eid' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45117**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'fdid' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45118**	N/A	A-PRO-ONLI-160124/509
Improper Neutralization of Special Elements used in an SQL Command	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'n' parameter of	N/A	A-PRO-ONLI-160124/510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45119**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'qid' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45120**	N/A	A-PRO-ONLI-160124/511
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'desc' parameter of the update.php	N/A	A-PRO-ONLI-160124/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45121**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'name' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45122**	N/A	A-PRO-ONLI-160124/513
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'right' parameter of the update.php resource does not	N/A	A-PRO-ONLI-160124/514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45123**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'tag' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45124**	N/A	A-PRO-ONLI-160124/515
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'time' parameter of the update.php resource does not validate the	N/A	A-PRO-ONLI-160124/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45125**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'total' parameter of the update.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-45126**	N/A	A-PRO-ONLI-160124/517
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	8.8	Online Examination System v1.0 is vulnerable to multiple Authenticated SQL Injection vulnerabilities. The 'wrong' parameter of the update.php resource does not validate the characters received	N/A	A-PRO-ONLI-160124/518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and they are sent unfiltered to the database. **CVE ID : CVE-2023-45127**		
Product: online_matrimonial_project					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'filename' attribute of the 'pic3' multipart parameter of the functions.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-46791**	N/A	A-PRO-ONLI-160124/519
Product: online_voting_system_project					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL	20-Dec-2023	9.8	Online Voting System Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The	N/A	A-PRO-ONLI-160124/520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			'username' parameter of the login_action.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48433**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Online Voting System Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the reg_action.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48434**	N/A	A-PRO-ONLI-160124/521
Product: railway_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an	21-Dec-2023	9.8	Railway Reservation System v1.0 is vulnerable to multiple Unauthenticated	N/A	A-PRO-RAIL-160124/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			SQL Injection vulnerabilities. The 'psd' parameter of the login.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48685**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Railway Reservation System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'user' parameter of the login.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48686**	N/A	A-PRO-RAIL-160124/523
Improper Neutralization of Special Elements used in an SQL	21-Dec-2023	9.8	Railway Reservation System v1.0 is vulnerable to multiple Unauthenticated SQL Injection	N/A	A-PRO-RAIL-160124/524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			vulnerabilities. The 'from' parameter of the reservation.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48687**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Railway Reservation System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'to' parameter of the reservation.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48688**	N/A	A-PRO-RAIL-160124/525
Improper Neutralization of Special Elements used in an	21-Dec-2023	9.8	Railway Reservation System v1.0 is vulnerable to multiple Unauthenticated	N/A	A-PRO-RAIL-160124/526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			SQL Injection vulnerabilities. The 'byname' parameter of the train.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48689**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Railway Reservation System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'bynum' parameter of the train.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48690**	N/A	A-PRO-RAIL-160124/527
Product: student_result_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	21-Dec-2023	9.8	Student Result Management System v1.0 is vulnerable to	N/A	A-PRO-STUD-160124/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			multiple Unauthenticated SQL Injection vulnerabilities. The 'class_id' parameter of the add_classes.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48716**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Student Result Management System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'class_name' parameter of the add_classes.php resource does not validate the characters received and they are sent unfiltered to the database. **CVE ID : CVE-2023-48717**	N/A	A-PRO-STUD-160124/529
Vendor: Putty					
Product: putty					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 0.80					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-PUT-PUTT-160124/530

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: quanticedge					
Product: first_order_discount_woocommerce					
Affected Version(s): * Up to (including) 1.21					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in QuanticEdge First Order Discount Woocommerce.This issue affects First Order Discount Woocommerce: from n/a through 1.21. **CVE ID : CVE-2023-49843**	N/A	A-QUA-FIRS-160124/531
Vendor: quantumcloud					
Product: ai_chatbot					
Affected Version(s): * Up to (including) 4.7.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in QuantumCloud AI ChatBot.This issue affects AI ChatBot: from n/a through 4.7.8. **CVE ID : CVE-2023-48741**	N/A	A-QUA-AI_C-160124/532
Vendor: quick-plugins					
Product: loan_repayment_calculator_and_application_form					
Affected Version(s): * Up to (including) 2.9.3					
Improper Neutralizat	21-Dec-2023	4.8	Improper Neutralization of	N/A	A-QUI-LOAN-160124/533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aerin Loan Repayment Calculator and Application Form allows Stored XSS.This issue affects Loan Repayment Calculator and Application Form: from n/a through 2.9.3. **CVE ID : CVE-2023-50829**		
Vendor: quttera					
Product: quttera_web_malware_scanner					
Affected Version(s): * Up to (excluding) 3.4.2.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	7.2	IThe Quttera Web Malware Scanner WordPress plugin before 3.4.2.1 does not validate user input used in a path, which could allow users with an admin role to perform path traversal attacks **CVE ID : CVE-2023-6222**	N/A	A-QUT-QUTT-160124/534
N/A	18-Dec-2023	5.3	The Quttera Web Malware Scanner WordPress plugin before 3.4.2.1	N/A	A-QUT-QUTT-160124/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			doesn't restrict access to detailed scan logs, which allows a malicious actor to discover local paths and portions of the site's code **CVE ID : CVE-2023-6065**		
Vendor: rajarora795					
Product: recently_viewed_products					
Affected Version(s): * Up to (including) 1.0.0					
Deserialization of Untrusted Data	19-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in Rajnish Arora Recently Viewed Products.This issue affects Recently Viewed Products: from n/a through 1.0.0. **CVE ID : CVE-2023-34027**	N/A	A-RAJ-RECE-160124/536
Vendor: Redhat					
Product: advanced_cluster_security					
Affected Version(s): 3.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50	A-RED-ADVA-160124/537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-	bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Affected Version(s): 4.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.c	A-RED-ADVA-160124/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in	om/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: ansible_automation_platform					
Affected Version(s): 1.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	A-RED-ANSI-160124/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	A-RED-ANSI-160124/540
Affected Version(s): 2.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	A-RED-ANSI-160124/541
Product: ansible_developer					
Affected Version(s): 1.0					
Improper Limitation of a Pathname to a	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw	https://access.redhat.com/errata/RHSA-2023:5701, https://access.r	A-RED-ANSI-160124/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	edhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	
Affected Version(s): 1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	A-RED-ANSI-160124/543
Product: ansible_inside					
Affected Version(s): 1.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/secu	A-RED-ANSI-160124/544

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file outside of the extraction path. **CVE ID : CVE-2023-5115**	rity/cve/CVE-2023-5115	
Affected Version(s): 1.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	A-RED-ANSI-160124/545
Product: ceph_storage					
Affected Version(s): 6.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627	A-RED-CEPH-160124/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypt	bf0a6f01c1f69e8ef1d4f05d	

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			o before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: cert-manager_operator_for_red_hat_openshift					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-CERT-160124/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: data_grid					
Affected Version(s): * Up to (excluding) 8.4.4					
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST. Bulk read endpoints do not properly evaluate user permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions. **CVE ID : CVE-2023-3628**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-3628	A-RED-DATA-160124/548
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST, Cache retrieval endpoints do not properly evaluate the necessary admin permissions	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/secu	A-RED-DATA-160124/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for the operation. This issue could allow an authenticated user to access information outside of their intended permissions. **CVE ID : CVE-2023-3629**	rity/cve/CVE-2023-3629	
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan, which does not detect circular object references when unmarshalling. An authenticated attacker with sufficient permissions could insert a maliciously constructed object into the cache and use it to cause out of memory errors and achieve a denial of service. **CVE ID : CVE-2023-5236**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-5236	A-RED-DATA-160124/550
Affected Version(s): * Up to (excluding) 8.4.6					
Cleartext Storage of Sensitive Information	18-Dec-2023	2.7	A flaw was found in Infinispan. When serializing the configuration for a cache to XML/JSON/YAML, which contains credentials (JDBC store with connection pooling, remote store), the	https://access.redhat.com/errata/RHSA-2023:7676, https://access.redhat.com/security/cve/CVE-2023-5384	A-RED-DATA-160124/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials are returned in clear text as part of the configuration. **CVE ID : CVE-2023-5384**		
Product: discovery					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-DISC-160124/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: jboss_data_grid					
Affected Version(s): -					
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST. Bulk read endpoints do not properly evaluate user permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions. **CVE ID : CVE-2023-3628**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-3628	A-RED-JBOS-160124/553
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST, Cache retrieval endpoints do not properly evaluate the necessary admin permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions. **CVE ID : CVE-2023-3629**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-3629	A-RED-JBOS-160124/554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan, which does not detect circular object references when unmarshalling. An authenticated attacker with sufficient permissions could insert a maliciously constructed object into the cache and use it to cause out of memory errors and achieve a denial of service. **CVE ID : CVE-2023-5236**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-5236	A-RED-JBOS-160124/555
Cleartext Storage of Sensitive Information	18-Dec-2023	2.7	A flaw was found in Infinispan. When serializing the configuration for a cache to XML/JSON/YAML, which contains credentials (JDBC store with connection pooling, remote store), the credentials are returned in clear text as part of the configuration. **CVE ID : CVE-2023-5384**	https://access.redhat.com/errata/RHSA-2023:7676, https://access.redhat.com/security/cve/CVE-2023-5384	A-RED-JBOS-160124/556
Product: jboss_enterprise_application_platform					
Affected Version(s): 6					
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST. Bulk read endpoints do not	https://access.redhat.com/errata/RHSA-2023:5396,	A-RED-JBOS-160124/557

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			properly evaluate user permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions. **CVE ID : CVE-2023-3628**	https://access.redhat.com/security/cve/CVE-2023-3628	
N/A	18-Dec-2023	6.5	A flaw was found in Infinispan's REST, Cache retrieval endpoints do not properly evaluate the necessary admin permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions. **CVE ID : CVE-2023-3629**	https://access.redhat.com/errata/RHSA-2023:5396, https://access.redhat.com/security/cve/CVE-2023-3629	A-RED-JBOS-160124/558
Affected Version(s): 7.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50	A-RED-JBOS-160124/559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-	bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: keycloak					
Affected Version(s): -					
URL Redirection to Untrusted Site ('Open Redirect')	18-Dec-2023	6.1	A flaw was found in Keycloak. This issue may allow an attacker to steal authorization codes or tokens from clients using a wildcard in the JARM response mode "form_post.jwt" which could be used to bypass the	https://access.redhat.com/security/cve/CVE-2023-6927, https://bugzilla.redhat.com/show_bug.cgi?id=2255027	A-RED-KEYC-160124/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security patch implemented to address CVE-2023-6134. **CVE ID : CVE-2023-6927**		
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-KEYC-160124/561

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48795		
Product: openshift_api_for_data_protection					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-OPEN-160124/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: openshift_container_platform					
Affected Version(s): 4.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-OPEN-160124/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		

Product: openshift_data_foundation

Affected Version(s): 4.0

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-OPEN-160124/564

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: openshift_developer_tools_and_services					
Affected Version(s): -					
Improper Validation of Integrity	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH	https://github.com/openssh/openssh-	A-RED-OPEN-160124/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Check Value			extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC	portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: openshift_dev_spaces					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other	https://github.com/openssh/openssh-portable/commits/master, https://github.c	A-RED-OPEN-160124/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms.	om/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: openshift_gitops					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad6760	A-RED-OPEN-160124/567

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API	1169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: openshift_pipelines					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.	A-RED-OPEN-160124/568

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through	xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: openshift_serverless					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/cry	A-RED-OPEN-160124/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP,	pto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: openshift_virtualization					
Affected Version(s): 4					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627	A-RED-OPEN-160124/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2,	bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: openstack_platform					
Affected Version(s): 16.1					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-OPEN-160124/571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Affected Version(s): 16.2					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack.	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-OPEN-160124/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Affected Version(s): 17.1					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP),	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-RED-OPEN-160124/573

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: satellite					
Affected Version(s): * Up to (excluding) 6.13					
Insufficient Session Expiration	18-Dec-2023	7.5	An arithmetic overflow flaw was found in Satellite when creating a new personal access token. This flaw allows an attacker who uses this arithmetic overflow to create personal access tokens that are valid indefinitely, resulting in damage to the system's integrity. **CVE ID : CVE-2023-4320**	https://access.redhat.com/security/cve/CVE-2023-4320	A-RED-SATE-160124/574
Product: service_interconnect					
Affected Version(s): 1.0					
Missing Authorization	18-Dec-2023	4.1	A flaw was found in the Skupper operator, which may permit a certain configuration to create a service account that would allow an authenticated	https://access.redhat.com/errata/RHSA-2023:6219, https://access.redhat.com/security/cve/CVE-2023-5056	A-RED-SERV-160124/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker in the adjacent cluster to view deployments in all namespaces in the cluster. This issue permits unauthorized viewing of information outside of the user's purview. **CVE ID : CVE-2023-5056**		
Product: single_sign-on					
Affected Version(s): 7.0					
URL Redirection to Untrusted Site ('Open Redirect')	18-Dec-2023	6.1	A flaw was found in Keycloak. This issue may allow an attacker to steal authorization codes or tokens from clients using a wildcard in the JARM response mode "form_post.jwt" which could be used to bypass the security patch implemented to address CVE-2023-6134. **CVE ID : CVE-2023-6927**	https://access.redhat.com/security/cve/CVE-2023-6927, https://bugzilla.redhat.com/show_bug.cgi?id=2255027	A-RED-SING-160124/576
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f	A-RED-SING-160124/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy	1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: storage					
Affected Version(s): 3.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh	A-RED-STOR-160124/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT,	/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: redpanda					
Product: redpanda					
Affected Version(s): * Up to (excluding) 23.1.21					
Missing Authorization	18-Dec-2023	9.8	Redpanda before 23.1.21 and 23.2.x before 23.2.18 has missing authorization checks in the Transactions API. **CVE ID : CVE-2023-50976**	https://github.com/redpanda-data/redpanda/pull/14969, https://github.com/redpanda-data/redpanda/pull/15060	A-RED-REDP-160124/579
Affected Version(s): From (including) 23.2.0 Up to (excluding) 23.2.18					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	18-Dec-2023	9.8	Redpanda before 23.1.21 and 23.2.x before 23.2.18 has missing authorization checks in the Transactions API. **CVE ID : CVE-2023-50976**	https://github.com/redpanda-data/redpanda/pull/14969, https://github.com/redpanda-data/redpanda/pull/15060	A-RED-REDP-160124/580
Vendor: remyandrade					
Product: school_visitor_log_e-book					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2023	5.4	A vulnerability was found in SourceCodester School Visitor Log e-Book 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file log-book.php. The manipulation of the argument Full Name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-248750 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-7059**	N/A	A-REM-SCHO-160124/581
Vendor: reviewsignal					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wpperformancetester					
Affected Version(s): * Up to (including) 2.0.0					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Kevin Ohashi WPPerformanceTester.This issue affects WPPerformanceTester: from n/a through 2.0.0. **CVE ID : CVE-2023-49844**	N/A	A-REV-WPPE-160124/582
Vendor: rmountjoy92					
Product: dashmachine					
Affected Version(s): 0.5-4					
Improper Control of Generation of Code ('Code Injection')	17-Dec-2023	9.8	A vulnerability classified as problematic was found in rmountjoy92 DashMachine 0.5-4. Affected by this vulnerability is an unknown functionality of the file /settings/save_config of the component Config Handler. The manipulation of the argument value_template leads to code injection. The exploit has been disclosed to the	N/A	A-RMO-DASH-160124/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. The identifier VDB-248257 was assigned to this vulnerability. **CVE ID : CVE-2023-6899**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	9.1	A vulnerability, which was classified as critical, has been found in rmountjoy92 DashMachine 0.5-4. Affected by this issue is some unknown functionality of the file /settings/delete_file. The manipulation of the argument file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-248258 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-6900**	N/A	A-RMO-DASH-160124/584
Vendor: roumenpetrov					
Product: pkixssh					
Affected Version(s): * Up to (excluding) 14.4					
Improper Validation of Integrity	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before	https://github.com/openssh/openssh-portable/commits/master,	A-ROU-PKIX-160124/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Check Value		🟨	9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com	https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: russh_project					
Product: russh					
Affected Version(s): * Up to (excluding) 0.40.2					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other	https://github.com/openssh/openssh-portable/commits/master, https://github.c	A-RUS-RUSS-160124/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms.	om/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: S-cms					
Product: S-cms					
Affected Version(s): 5.0					
Improper Neutralization of Special Elements used in an SQL	21-Dec-2023	9.8	S-CMS v5.0 was discovered to contain a SQL injection vulnerability via the A_newsauth	N/A	A-S-C-S-CM-160124/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			parameter at /admin/ajax.php. **CVE ID : CVE-2023-51048**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	S-CMS v5.0 was discovered to contain a SQL injection vulnerability via the A_bbsauth parameter at /admin/ajax.php. **CVE ID : CVE-2023-51049**	N/A	A-S-C-S-CM-160124/588
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	S-CMS v5.0 was discovered to contain a SQL injection vulnerability via the A_productauth parameter at /admin/ajax.php. **CVE ID : CVE-2023-51050**	N/A	A-S-C-S-CM-160124/589
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	S-CMS v5.0 was discovered to contain a SQL injection vulnerability via the A_textauth parameter at /admin/ajax.php. **CVE ID : CVE-2023-51051**	N/A	A-S-C-S-CM-160124/590
Improper Neutralization of Special Elements used in an SQL	21-Dec-2023	9.8	S-CMS v5.0 was discovered to contain a SQL injection vulnerability via the A_formauth	N/A	A-S-C-S-CM-160124/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			parameter at /admin/ajax.php. **CVE ID : CVE-2023-51052**		
Vendor: saintsystems					
Product: disable_user_login					
Affected Version(s): * Up to (including) 1.3.7					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Saint Systems Disable User Login.This issue affects Disable User Login: from n/a through 1.3.7. **CVE ID : CVE-2023-47806**	N/A	A-SAI-DISA-160124/592
Vendor: sajjadhsagor					
Product: wp_edit_username					
Affected Version(s): * Up to (including) 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sajjad Hossain Sagor WP Edit Username allows Stored XSS.This issue affects WP Edit Username: from n/a through 1.0.5.	N/A	A-SAJ-WP_E-160124/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-47527		
Vendor: saurabhspeaks					
Product: advanced_category_template					
Affected Version(s): * Up to (including) 0.1					
Cross-Site Request Forgery (CSRF)	19-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Praveen Goswami Advanced Category Template.This issue affects Advanced Category Template: from n/a through 0.1. **CVE ID : CVE-2023-50835**	N/A	A-SAU-ADVA-160124/594
Vendor: sentry					
Product: astro					
Affected Version(s): From (including) 7.78.0 Up to (excluding) 7.87.0					
N/A	20-Dec-2023	7.5	Sentry-Javascript is official Sentry SDKs for JavaScript. A ReDoS (Regular expression Denial of Service) vulnerability has been identified in Sentry's Astro SDK 7.78.0-7.86.0. Under certain conditions, this vulnerability allows an attacker to cause excessive computation times on the server,	https://github.com/getsentry/sentry-javascript/security/advisories/GHSA-x3v3-8xg8-8v72, https://github.com/getsentry/sentry-javascript/pull/9815, https://github.com/getsentry/sentry-javascript/commit/fe24eb5eef	A-SEN-ASTR-160124/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leading to denial of service (DoS). This vulnerability has been patched in sentry/astro version 7.87.0. **CVE ID : CVE-2023-50249**	a9d27b14b2b6f9ebd1debca1c208fb	
Vendor: seosthemes					
Product: seos_contact_form					
Affected Version(s): * Up to (including) 1.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	4.8	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Seosbg Seos Contact Form allows Stored XSS.This issue affects Seos Contact Form: from n/a through 1.8.0. **CVE ID : CVE-2023-50830**	N/A	A-SEO-SEOS-160124/596
Vendor: servit					
Product: affiliate-toolkit_-_wordpress_affiliate					
Affected Version(s): * Up to (including) 3.3.9					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2023	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in SERVIT Software Solutions affiliate-toolkit – WordPress Affiliate	N/A	A-SER-AFFI-160124/597

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plugin.This issue affects affiliate-toolkit – WordPress Affiliate Plugin: from n/a through 3.3.9. **CVE ID : CVE-2023-45105**		
Vendor: sftpgo_project					
Product: sftpgo					
Affected Version(s): * Up to (excluding) 2.5.6					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP),	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-SFT-SFTP-160124/598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: sigmaplugin					
Product: advanced_database_cleaner					
Affected Version(s): * Up to (including) 3.1.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Younes JFR. Advanced Database Cleaner.This issue affects Advanced Database Cleaner: from n/a through 3.1.2. **CVE ID : CVE-2023-49764**	N/A	A-SIG-ADVA-160124/599
Vendor: simple-membership-plugin					
Product: simple_membership					
Affected Version(s): * Up to (including) 4.3.8					
Improper Neutralization of Input During Web Page Generation	19-Dec-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	N/A	A-SIM-SIMP-160124/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			smp7, wp.Insider Simple Membership allows Reflected XSS.This issue affects Simple Membership: from n/a through 4.3.8. **CVE ID : CVE-2023-50376**		
Vendor: siteorigin					
Product: siteorigin_widgets_bundle					
Affected Version(s): * Up to (excluding) 1.51.0					
N/A	18-Dec-2023	7.2	The SiteOrigin Widgets Bundle WordPress plugin before 1.51.0 does not validate user input before using it to generate paths passed to include function/s, allowing users with the administrator role to perform LFI attacks in the context of Multisite WordPress sites. **CVE ID : CVE-2023-6295**	N/A	A-SIT-SITE-160124/601
Vendor: Smackcoders					
Product: export_all_posts\,_products\,_orders\,_refunds_\&_users					
Affected Version(s): * Up to (including) 2.4.1					
Exposure of Sensitive Information to an Unauthorized Actor	21-Dec-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Smackcoders	N/A	A-SMA-EXPO-160124/602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Export All Posts, Products, Orders, Refunds & Users.This issue affects Export All Posts, Products, Orders, Refunds & Users: from n/a through 2.4.1. **CVE ID : CVE-2023-2487**		
Vendor: soflyy					
Product: export_any_wordpress_data_to_xml\/csv					
Affected Version(s): * Up to (excluding) 1.4.0					
N/A	18-Dec-2023	7.2	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not validate and sanitise the `wp_query` parameter which allows an attacker to run arbitrary command on the remote server **CVE ID : CVE-2023-4724**	N/A	A-SOF-EXPO-160124/603
Affected Version(s): * Up to (excluding) 1.4.1					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro	N/A	A-SOF-EXPO-160124/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WordPress plugin before 1.8.6 does not check nonce tokens early enough in the request lifecycle, allowing attackers to make logged in users perform unwanted actions leading to remote code execution. **CVE ID : CVE-2023-5882**		
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not check nonce tokens early enough in the request lifecycle, allowing attackers with the ability to upload files to make logged in users perform unwanted actions leading to PHAR deserialization, which may lead to remote code execution. **CVE ID : CVE-2023-5886**	N/A	A-SOF-EXPO-160124/605
Product: wp_all_export					
Affected Version(s): * Up to (excluding) 1.8.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not check nonce tokens early enough in the request lifecycle, allowing attackers to make logged in users perform unwanted actions leading to remote code execution. **CVE ID : CVE-2023-5882**	N/A	A-SOF-WP_A-160124/606
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not check nonce tokens early enough in the request lifecycle, allowing attackers with the ability to upload files to make logged in users perform unwanted actions leading to PHAR deserialization, which may lead to remote code execution.	N/A	A-SOF-WP_A-160124/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5886		
N/A	18-Dec-2023	7.2	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not validate and sanitise the \`wp_query\` parameter which allows an attacker to run arbitrary command on the remote server **CVE ID : CVE-2023-4724**	N/A	A-SOF-WP_A-160124/608
Vendor: Softing					
Product: edgeaggregator					
Affected Version(s): 3.4.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Dec-2023	7.2	Softing edgeAggregator Restore Configuration Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Softing edgeAggregator. Authentication is required to exploit this vulnerability.	N/A	A-SOF-EDGE-160124/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The specific flaw exists within the processing of backup zip files. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this to execute code in the context of root. Was ZDI-CAN-20543. **CVE ID : CVE-2023-38126**		
Vendor: softlabbd					
Product: integrate_google_drive					
Affected Version(s): * Up to (excluding) 1.3.5					
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.4. **CVE ID : CVE-2023-49769**	N/A	A-SOF-INTE-160124/610
Vendor: softomi					
Product: advanced_c2c_marketplace_software					
Affected Version(s): * Up to (excluding) 12122023					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ?stanbul Soft Informatics and Consultancy Limited Company Softomi Advanced C2C Marketplace Software allows SQL Injection.This issue affects Softomi Advanced C2C Marketplace Software: before 12122023. **CVE ID : CVE-2023-6145**	N/A	A-SOF-ADVA-160124/611
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	6.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ?stanbul Soft Informatics and Consultancy Limited Company Softomi Geli?mi? C2C Pazaryeri Yaz?l?m? allows Reflected XSS.This issue affects Softomi Geli?mi? C2C Pazaryeri	N/A	A-SOF-ADVA-160124/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Yaz?l?m?: before 12122023. **CVE ID : CVE-2023-6122**		
Vendor: spoonthemes					
Product: adifier					
Affected Version(s): * Up to (excluding) 3.1.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spoon themes Adifier - Classified Ads WordPress Theme.This issue affects Adifier - Classified Ads WordPress Theme: from n/a before 3.1.4. **CVE ID : CVE-2023-49752**	N/A	A-SPO-ADIF-160124/613
Product: couponis					
Affected Version(s): * Up to (excluding) 2.2					
Improper Neutralization of Special Elements used in an SQL Command	19-Dec-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spoonthemes Couponis - Affiliate	N/A	A-SPO-COUP-160124/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			& Submitting Coupons WordPress Theme.This issue affects Couponis - Affiliate & Submitting Coupons WordPress Theme: from n/a before 2.2. **CVE ID : CVE-2023-49750**		
Vendor: SSH					
Product: ssh					
Affected Version(s): * Up to (excluding) 5.11					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-SSH-SSH-160124/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: ssh2_project					
Product: ssh2					
Affected Version(s): * Up to (including) 1.11.0					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack.	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-SSH-SSH2-160124/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: starnight					
Product: micro_http_server					
Affected Version(s): -					
Out-of-bounds Write	17-Dec-2023	9.8	In MicroHttpServer (aka Micro HTTP Server) through 4398570, _ReadStaticFiles in lib/middleware.c allows a stack-based buffer overflow and potentially remote code execution via a long URI. **CVE ID : CVE-2023-50965**	N/A	A-STA-MICR-160124/617
Vendor: stormshield					
Product: stormshield_network_security					
Affected Version(s): 4.7.0					
N/A	21-Dec-2023	6.5	An issue was discovered in Stormshield Network Security (SNS) 4.0.0 through 4.3.21, 4.4.0 through 4.6.8, and 4.7.0. Sending a	https://advisories.stormshield.eu/2023-031/	A-STO-STOR-160124/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted ICMP packet may lead to a crash of the ASQ engine. **CVE ID : CVE-2023-47093**		
Affected Version(s): From (including) 3.11.0 Up to (including) 3.11.27					
N/A	21-Dec-2023	5.3	An issue was discovered in Stormshield Network Security (SNS) 3.7.0 through 3.7.39, 3.11.0 through 3.11.27, 4.3.0 through 4.3.22, 4.6.0 through 4.6.9, and 4.7.0 through 4.7.1. It's possible to know if a specific user account exists on the SNS firewall by using remote access commands. **CVE ID : CVE-2023-41166**	https://advisories.stormshield.eu/2023-027	A-STO-STOR-160124/619
Affected Version(s): From (including) 3.7.0 Up to (including) 3.7.39					
N/A	21-Dec-2023	5.3	An issue was discovered in Stormshield Network Security (SNS) 3.7.0 through 3.7.39, 3.11.0 through 3.11.27, 4.3.0 through 4.3.22, 4.6.0 through 4.6.9, and 4.7.0 through 4.7.1. It's possible to know if a specific user account exists on the SNS firewall	https://advisories.stormshield.eu/2023-027	A-STO-STOR-160124/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			by using remote access commands. **CVE ID : CVE-2023-41166**		
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.3.22					
N/A	21-Dec-2023	6.5	An issue was discovered in Stormshield Network Security (SNS) 4.0.0 through 4.3.21, 4.4.0 through 4.6.8, and 4.7.0. Sending a crafted ICMP packet may lead to a crash of the ASQ engine. **CVE ID : CVE-2023-47093**	https://advisories.stormshield.eu/2023-031/	A-STO-STOR-160124/621
Affected Version(s): From (including) 4.3.0 Up to (excluding) 4.3.23					
N/A	21-Dec-2023	5.3	An issue was discovered in Stormshield Network Security (SNS) 3.7.0 through 3.7.39, 3.11.0 through 3.11.27, 4.3.0 through 4.3.22, 4.6.0 through 4.6.9, and 4.7.0 through 4.7.1. It's possible to know if a specific user account exists on the SNS firewall by using remote access commands. **CVE ID : CVE-2023-41166**	https://advisories.stormshield.eu/2023-027	A-STO-STOR-160124/622
Affected Version(s): From (including) 4.4.0 Up to (excluding) 4.6.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Dec-2023	6.5	An issue was discovered in Stormshield Network Security (SNS) 4.0.0 through 4.3.21, 4.4.0 through 4.6.8, and 4.7.0. Sending a crafted ICMP packet may lead to a crash of the ASQ engine. **CVE ID : CVE-2023-47093**	https://advisories.stormshield.eu/2023-031/	A-STO-STOR-160124/623
Affected Version(s): From (including) 4.6.0 Up to (excluding) 4.6.10					
N/A	21-Dec-2023	5.3	An issue was discovered in Stormshield Network Security (SNS) 3.7.0 through 3.7.39, 3.11.0 through 3.11.27, 4.3.0 through 4.3.22, 4.6.0 through 4.6.9, and 4.7.0 through 4.7.1. It's possible to know if a specific user account exists on the SNS firewall by using remote access commands. **CVE ID : CVE-2023-41166**	https://advisories.stormshield.eu/2023-027	A-STO-STOR-160124/624
Affected Version(s): From (including) 4.7.0 Up to (excluding) 4.7.2					
N/A	21-Dec-2023	5.3	An issue was discovered in Stormshield Network Security (SNS) 3.7.0 through 3.7.39, 3.11.0 through 3.11.27,	https://advisories.stormshield.eu/2023-027	A-STO-STOR-160124/625

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			4.3.0 through 4.3.22, 4.6.0 through 4.6.9, and 4.7.0 through 4.7.1. It's possible to know if a specific user account exists on the SNS firewall by using remote access commands. **CVE ID : CVE-2023-41166**		
Vendor: subscribe_to_category_project					
Product: subscribe_to_category					
Affected Version(s): * Up to (including) 2.7.4					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	7.5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Daniel Söderström / Sidney van de Stouwe Subscribe to Category.This issue affects Subscribe to Category: from n/a through 2.7.4. **CVE ID : CVE-2023-32590**	N/A	A-SUB-SUBS-160124/626
Vendor: sunshinephotocart					
Product: sunshine_photo_cart					
Affected Version(s): * Up to (excluding) 3.0					
Authorization Bypass Through	20-Dec-2023	6.5	Authorization Bypass Through User-Controlled	N/A	A-SUN-SUNS-160124/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User-Controlled Key			Key vulnerability in WP Sunshine Sunshine Photo Cart: Free Client Galleries for Photographers.This issue affects Sunshine Photo Cart: Free Client Galleries for Photographers: from n/a before 3.0.0. **CVE ID : CVE-2023-41796**		
Vendor: svgator					
Product: svgator					
Affected Version(s): * Up to (including) 1.2.4					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in SVGator SVGator – Add Animated SVG Easily.This issue affects SVGator – Add Animated SVG Easily: from n/a through 1.2.4. **CVE ID : CVE-2023-48766**	N/A	A-SVG-SVGA-160124/628
Vendor: swapnilpatil					
Product: login_and_logout_redirect					
Affected Version(s): * Up to (including) 2.0.3					
URL Redirectio	19-Dec-2023	6.1	URL Redirection to Untrusted Site	N/A	A-SWA-LOGI-160124/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n to Untrusted Site ('Open Redirect')			('Open Redirect') vulnerability in Swapnil V. Patil Login and Logout Redirect.This issue affects Login and Logout Redirect: from n/a through 2.0.3. **CVE ID : CVE-2023-41648**		
Vendor: swteplugins					
Product: swift_performance					
Affected Version(s): * Up to (excluding) 2.3.6.15					
N/A	18-Dec-2023	4.3	The Swift Performance Lite WordPress plugin before 2.3.6.15 does not prevent users from exporting the plugin's settings, which may include sensitive information such as Cloudflare API tokens. **CVE ID : CVE-2023-6289**	N/A	A-SWT-SWIF-160124/630
Vendor: symbiostock					
Product: symbiostock					
Affected Version(s): * Up to (including) 6.0.0					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	7.2	Unrestricted Upload of File with Dangerous Type vulnerability in Symbiostock symbiostock.This	N/A	A-SYM-SYMB-160124/631

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects Symbiostock: from n/a through 6.0.0. **CVE ID : CVE-2023-49814**		
Vendor: taggbox					
Product: taggbox					
Affected Version(s): * Up to (including) 3.1					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tagbox Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics.This issue affects Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics: from n/a through 3.1. **CVE ID : CVE-2023-33214**	N/A	A-TAG-TAGG-160124/632
Vendor: teachpress_project					
Product: teachpress					
Affected Version(s): * Up to (excluding) 9.0.5					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Michael Winkler teachPress.This issue affects	N/A	A-TEA-TEAC-160124/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			teachPress: from n/a through 9.0.4. **CVE ID : CVE-2023-48755**		
Vendor: tera_term_project					
Product: tera_term					
Affected Version(s): * Up to (including) 5.1					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-TER-TERA-160124/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: Thegreenbow					
Product: windows_enterprise_certified_vpn					
Affected Version(s): 6.52					
Improper Privilege Management	19-Dec-2023	9.8	An issue discovered in TheGreenBow Windows Enterprise Certified VPN Client 6.52, Windows Standard VPN Client 6.87, and Windows Enterprise VPN Client 6.87 allows attackers to gain escalated privileges via crafted changes to memory mapped file. **CVE ID : CVE-2023-47267**	https://www.thegreenbow.com/en/support/security-alerts/#deeplink-16093	A-THE-WIND-160124/635
Product: windows_enterprise_vpn					
Affected Version(s): 6.87					
Improper Privilege Management	19-Dec-2023	9.8	An issue discovered in TheGreenBow Windows Enterprise Certified VPN Client 6.52, Windows Standard VPN Client 6.87, and Windows Enterprise VPN	https://www.thegreenbow.com/en/support/security-alerts/#deeplink-16093	A-THE-WIND-160124/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Client 6.87 allows attackers to gain escalated privileges via crafted changes to memory mapped file. **CVE ID : CVE-2023-47267**		
Product: windows_standard_vpn					
Affected Version(s): 6.87					
Improper Privilege Management	19-Dec-2023	9.8	An issue discovered in TheGreenBow Windows Enterprise Certified VPN Client 6.52, Windows Standard VPN Client 6.87, and Windows Enterprise VPN Client 6.87 allows attackers to gain escalated privileges via crafted changes to memory mapped file. **CVE ID : CVE-2023-47267**	https://www.thegreenbow.com/en/support/security-alerts/#deeplink-16093	A-THE-WIND-160124/637
Vendor: themefic					
Product: ultimate_addons_for_contact_form_7					
Affected Version(s): * Up to (excluding) 3.1.24					
Improper Neutralization of Special Elements used in an SQL	20-Dec-2023	8.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	N/A	A-THE-ULTI-160124/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			Themefic Ultimate Addons for Contact Form 7.This issue affects Ultimate Addons for Contact Form 7: from n/a through 3.1.23. **CVE ID : CVE-2023-30495**		
Vendor: themely					
Product: theme_demo_import					
Affected Version(s): * Up to (including) 1.1.1					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	7.2	Unrestricted Upload of File with Dangerous Type vulnerability in Themely Theme Demo Import.This issue affects Theme Demo Import: from n/a through 1.1.1. **CVE ID : CVE-2023-28170**	N/A	A-THE-THEM-160124/639
Vendor: thememylogin					
Product: 2fa					
Affected Version(s): * Up to (excluding) 1.2					
Improper Restriction of Excessive Authentication Attempts	18-Dec-2023	9.8	The Theme My Login 2FA WordPress plugin before 1.2 does not rate limit 2FA validation attempts, which may allow an attacker to brute-	N/A	A-THE-2FA-160124/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			force all possibilities, which shouldn't be too long, as the 2FA codes are 6 digits. **CVE ID : CVE-2023-6272**		
Vendor: Themepunch					
Product: slider_revolution					
Affected Version(s): * Up to (including) 6.6.15					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in ThemePunch OHG Slider Revolution.This issue affects Slider Revolution: from n/a through 6.6.15. **CVE ID : CVE-2023-47784**	N/A	A-THE-SLID-160124/641
Vendor: themesflat					
Product: themesflat_addons_for_elementor					
Affected Version(s): * Up to (including) 2.0.0					
Deserialization of Untrusted Data	19-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in Themesflat Themesflat Addons For Elementor.This issue affects Themesflat Addons For Elementor: from n/a through 2.0.0.	N/A	A-THE-THEM-160124/642

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-37390		
Vendor: themify					
Product: themify_ultra					
Affected Version(s): * Up to (excluding) 7.3.6					
Deserialization of Untrusted Data	20-Dec-2023	8.8	Deserialization of Untrusted Data vulnerability in Themify Themify Ultra.This issue affects Themify Ultra: from n/a through 7.3.5. **CVE ID : CVE-2023-46147**	N/A	A-THE-THEM-160124/643
Product: ultra					
Affected Version(s): * Up to (including) 7.3.5					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in Themify Themify Ultra.This issue affects Themify Ultra: from n/a through 7.3.5. **CVE ID : CVE-2023-46149**	N/A	A-THE-ULTR-160124/644
Vendor: tinyssh					
Product: tinyssh					
Affected Version(s): * Up to (including) 20230101					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-TIN-TINY-160124/645

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: tongda2000					
Product: office_anywhere_2017					
Affected Version(s): * Up to (including) 11.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	A vulnerability was found in Tongda OA 2017 up to 11.9. It has been classified as critical. Affected is an unknown function of the file general/vehicle/checkup/delete_search.php. The manipulation of the argument VU_ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248568. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7021**	N/A	A-TON-OFFI-160124/646
Affected Version(s): * Up to (including) 11.9					
Improper Neutralizat	21-Dec-2023	9.8	A vulnerability was found in Tongda	N/A	A-TON-OFFI-160124/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			OA 2017 up to 11.9 and classified as critical. This issue affects some unknown processing of the file general/wiki/cp/ct/view.php. The manipulation of the argument TEMP_ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-248567. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7020**		
Improper Neutralization of Special Elements	21-Dec-2023	9.8	A vulnerability was found in Tongda OA 2017 up to 11.9. It has been declared as critical.	N/A	A-TON-OFFI-160124/648

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			Affected by this vulnerability is an unknown functionality of the file general/work_plan/manage/delete_all.php. The manipulation of the argument DELETE_STR leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248569 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-7022**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Dec-2023	9.8	A vulnerability was found in Tongda OA 2017 up to 11.9. It has been rated as critical. Affected by this issue is some unknown functionality of the file general/vehicle/query/delete.php. The manipulation	N/A	A-TON-OFFI-160124/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument VU_ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-248570 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-2023-7023**		
Product: tongda_office_anywhere					
Affected Version(s): * Up to (including) 11.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Dec-2023	9.8	A vulnerability was found in Tongda OA 2017 up to 11.10. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file general/vote/manage/delete.php. The manipulation	N/A	A-TON-TONG-160124/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-248245 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6885**		
Affected Version(s): 2017					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Dec-2023	9.8	A vulnerability was found in Tongda OA 2017 up to 11.10. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file general/vote/manage/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-248245 was assigned to this vulnerability. NOTE: The vendor	N/A	A-TON-TONG-160124/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6885**		
Vendor: tri					
Product: the_events_calendar					
Affected Version(s): * Up to (excluding) 6.2.8.1					
N/A	18-Dec-2023	7.5	The Events Calendar WordPress plugin before 6.2.8.1 discloses the content of password protected posts to unauthenticated users via a crafted request **CVE ID : CVE-2023-6203**	N/A	A-TRI-THE_-160124/652
Vendor: Tribulant					
Product: slideshow_gallery					
Affected Version(s): * Up to (including) 1.7.6					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tribulant Slideshow Gallery LITE.This issue affects Slideshow Gallery LITE: from n/a through 1.7.6.	N/A	A-TRI-SLID-160124/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28491		
Vendor: trilead					
Product: ssh2					
Affected Version(s): 6401					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-TRI-SSH2-160124/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48795		
Vendor: unlimited-elements					
Product: unlimited_elements_for_elementor_\(free_widgets\,_addons\,_templates\)					
Affected Version(s): * Up to (excluding) 1.5.66					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	6.5	Unrestricted Upload of File with Dangerous Type vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates).This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 1.5.65. **CVE ID : CVE-2023-31231**	N/A	A-UNL-UNLI-160124/655
Vendor: Unrealircd					
Product: unrealircd					
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.4					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Dec-2023	7.5	A buffer overflow in websockets in UnrealIRCd 6.1.0 through 6.1.3 before 6.1.4 allows an unauthenticated remote attacker to crash the server by sending an oversized packet (if	https://forums.unrealircd.org/viewtopic.php?t=9340	A-UNR-UNRE-160124/656

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a websocket port is open). Remote code execution might be possible on some uncommon, older platforms. **CVE ID : CVE-2023-50784**		
Vendor: uxthemes					
Product: flatsome					
Affected Version(s): * Up to (excluding) 3.17.6					
Deserialization of Untrusted Data	20-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in UX-themes Flatsome | Multi-Purpose Responsive WooCommerce Theme.This issue affects Flatsome | Multi-Purpose Responsive WooCommerce Theme: from n/a through 3.17.5. **CVE ID : CVE-2023-40555**	N/A	A-UXT-FLAT-160124/657
Vendor: Vandyke					
Product: securecrt					
Affected Version(s): * Up to (excluding) 9.4.3					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/	A-VAN-SECU-160124/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects	blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: villatheme					
Product: curcy					
Affected Version(s): * Up to (including) 2.2.0					
Improper Neutralization of Input During Web Page Generation	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VillaTheme CURCY	N/A	A-VIL-CURC-160124/659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			– Multi Currency for WooCommerce allows Stored XSS.This issue affects CURCY – Multi Currency for WooCommerce: from n/a through 2.2.0. **CVE ID : CVE-2023-50831**		
Product: product_size_chart_for_woocommerce					
Affected Version(s): * Up to (including) 1.1.5					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in VillaTheme Product Size Chart For WooCommerce.This issue affects Product Size Chart For WooCommerce: from n/a through 1.1.5. **CVE ID : CVE-2023-48778**	N/A	A-VIL-PROD-160124/660
Vendor: wang.market					
Product: wangmarket					
Affected Version(s): 6.1					
Improper Control of Generation of Code	17-Dec-2023	9.8	A vulnerability was found in xnx3 wangmarket 6.1. It has been rated as critical. Affected by	N/A	A-WAN-WANG-160124/661

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			this issue is some unknown functionality of the component Role Management Page. The manipulation leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-248246 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-6886**		
Vendor: wcvendors					
Product: woocommerce_multi-vendor\,_woocommerce_marketplace\,_product_vendors					
Affected Version(s): * Up to (including) 2.4.7					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WC Vendors WC Vendors – WooCommerce Multi-Vendor, WooCommerce Marketplace, Product Vendors.This issue affects WC Vendors – WooCommerce Multi-Vendor, WooCommerce	N/A	A-WCV-WOOC-160124/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Marketplace, Product Vendors: from n/a through 2.4.7. **CVE ID : CVE-2023-48327**		
Vendor: web-soudan					
Product: mw_wp_form					
Affected Version(s): * Up to (excluding) 5.0.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Dec-2023	9.8	The MW WP Form plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to, and including, 5.0.3. This is due to the plugin not properly validating the path of an uploaded file prior to deleting it. This makes it possible for unauthenticated attackers to delete arbitrary files, including the wp-config.php file, which can make site takeover and remote code execution possible. **CVE ID : CVE-2023-6559**	https://www.wordfence.com/threat-intel/vulnerabilities/id/412d555c-9bbd-42f5-8020-ccfc18755a79?source=cve, https://plugins.trac.wordpress.org/changeset/3007879/mw-wp-form	A-WEB-MW_W-160124/663
Vendor: webbjocke					
Product: simple_wp_sitemap					
Affected Version(s): * Up to (including) 1.2.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Webbjocke Simple Wp Sitemap.This issue affects Simple Wp Sitemap: from n/a through 1.2.1. **CVE ID : CVE-2023-24380**	N/A	A-WEB-SIMP-160124/664
Vendor: wedevs					
Product: dokan					
Affected Version(s): * Up to (excluding) 3.7.13					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	8.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs Dokan – Best WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy.This issue affects Dokan – Best WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy: from n/a through 3.7.12.	N/A	A-WED-DOKA-160124/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26525		
Affected Version(s): * Up to (including) 3.7.19					
Deserialization of Untrusted Data	19-Dec-2023	8.8	Deserialization of Untrusted Data vulnerability in weDevs Dokan – Best WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy.This issue affects Dokan – Best WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy: from n/a through 3.7.19. **CVE ID : CVE-2023-34382**	N/A	A-WED-DOKA-160124/666
Vendor: whereyoursolutionis					
Product: fix_my_feed_rss_repair					
Affected Version(s): * Up to (including) 1.4					
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Innovative Solutions Fix My Feed RSS Repair.This issue affects Fix My Feed RSS Repair: from n/a through 1.4.	N/A	A-WHE-FIX_-160124/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49816		
Vendor: Winscp					
Product: winscp					
Affected Version(s): * Up to (excluding) 6.2.2					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	A-WIN-WINS-160124/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: winwar					
Product: wp_email_capture					
Affected Version(s): * Up to (excluding) 3.11					
Exposure of Sensitive Information to an Unauthorized Actor	21-Dec-2023	7.5	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Winwar Media WordPress Email Marketing Plugin – WP Email Capture.This issue affects WordPress Email Marketing Plugin – WP Email Capture: from n/a through 3.10. **CVE ID : CVE-2023-28421**	N/A	A-WIN-WP_E-160124/669
Vendor: wipeoutmedia					
Product: css_\&_javascript_toolbox					
Affected Version(s): * Up to (including) 11.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2023	5.4	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wipeout Media CSS & JavaScript Toolbox allows Stored XSS.This	N/A	A-WIP-CSS_-160124/670

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue affects CSS & JavaScript Toolbox: from n/a through 11.7. **CVE ID : CVE-2023-50823**		
Vendor: woo					
Product: product_vendors					
Affected Version(s): * Up to (excluding) 2.1.77					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WooCommerce Product Vendors allows SQL Injection.This issue affects Product Vendors: from n/a through 2.1.76. **CVE ID : CVE-2023-33331**	N/A	A-WOO-PROD-160124/671
Vendor: Woocommerce					
Product: automatewoo					
Affected Version(s): * Up to (excluding) 4.9.51					
Improper Neutralization of Special Elements used in an SQL	20-Dec-2023	8.1	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	N/A	A-WOO-AUTO-160124/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			WooCommerce AutomateWoo.This issue affects AutomateWoo: from n/a through 4.9.50. **CVE ID : CVE-2023-33330**		
Affected Version(s): * Up to (excluding) 5.7.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Dec-2023	4.9	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WooCommerce AutomateWoo.This issue affects AutomateWoo: from n/a through 5.7.1. **CVE ID : CVE-2023-32743**	N/A	A-WOO-AUTO-160124/673
Affected Version(s): * Up to (including) 4.9.40					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in WooCommerce AutomateWoo.This issue affects AutomateWoo: from n/a through 4.9.40.	N/A	A-WOO-AUTO-160124/674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33318		
Product: shipping_multiple_addresses					
Affected Version(s): * Up to (including) 3.8.3					
Authorization Bypass Through User-Controlled Key	21-Dec-2023	6.5	Authorization Bypass Through User-Controlled Key vulnerability in WooCommerce Shipping Multiple Addresses.This issue affects Shipping Multiple Addresses: from n/a through 3.8.3. **CVE ID : CVE-2023-32799**	N/A	A-WOO-SHIP-160124/675
Vendor: woorockets					
Product: corsa					
Affected Version(s): * Up to (including) 1.5					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in WooRockets Corsa.This issue affects Corsa: from n/a through 1.5. **CVE ID : CVE-2023-23970**	N/A	A-WOO-CORS-160124/676
Vendor: wow-company					
Product: button_generator					
Affected Version(s): * Up to (including) 2.3.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Button Generator – easily Button Builder.This issue affects Button Generator – easily Button Builder: from n/a through 2.3.8. **CVE ID : CVE-2023-49155**	N/A	A-WOW-BUTT-160124/677
Vendor: wpchill					
Product: download_monitor					
Affected Version(s): * Up to (including) 4.8.3					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	Unrestricted Upload of File with Dangerous Type vulnerability in WPChill Download Monitor.This issue affects Download Monitor: from n/a through 4.8.3. **CVE ID : CVE-2023-34007**	N/A	A-WPC-DOWN-160124/678
Vendor: wpcore					
Product: csv_importer					
Affected Version(s): * Up to (including) 0.3.8					
Cross-Site Request Forgery (CSRF)	17-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Denis Kobozev CSV	N/A	A-WPC-CSV_-160124/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Importer.This issue affects CSV Importer: from n/a through 0.3.8. **CVE ID : CVE-2023-49775**		
Vendor: wpdoctor					
Product: woocommerce_login_redirect					
Affected Version(s): * Up to (including) 2.2.4					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in WP Doctor WooCommerce Login Redirect.This issue affects WooCommerce Login Redirect: from n/a through 2.2.4. **CVE ID : CVE-2023-48773**	N/A	A-WPD-WOOC-160124/680
Vendor: wpfoxly					
Product: adfoxly					
Affected Version(s): * Up to (including) 1.8.5					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in AdFoxly AdFoxly – Ad Manager, AdSense Ads & Ads.Txt.This issue affects AdFoxly – Ad Manager, AdSense Ads &	N/A	A-WPF-ADFO-160124/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ads.Txt: from n/a through 1.8.5. **CVE ID : CVE-2023-46617**		
Vendor: wpfrank					
Product: slider_factory_pro					
Affected Version(s): * Up to (excluding) 3.5.12					
N/A	18-Dec-2023	6.5	The Slider WordPress plugin before 3.5.12 does not ensure that posts to be accessed via an AJAX action are slides and can be viewed by the user making the request, allowing any authenticated users, such as subscriber to access the content arbitrary post such as private, draft and password protected **CVE ID : CVE-2023-6077**	N/A	A-WPF-SLID-160124/682
Vendor: wpgogo					
Product: custom_post_type_page_template					
Affected Version(s): * Up to (including) 1.1					
Cross-Site Request Forgery (CSRF)	18-Dec-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Hiroaki Miyashita Custom Post Type Page Template.This issue affects	N/A	A-WPG-CUST-160124/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Custom Post Type Page Template: from n/a through 1.1. **CVE ID : CVE-2023-50372**		
Vendor: wpmudev					
Product: smartcrawl					
Affected Version(s): * Up to (excluding) 3.8.3					
Missing Authorization	18-Dec-2023	7.5	The SmartCrawl WordPress plugin before 3.8.3 does not prevent unauthorised users from accessing password-protected posts' content. **CVE ID : CVE-2023-5949**	N/A	A-WPM-SMAR-160124/684
Vendor: wppa					
Product: wp_photo_album_plus					
Affected Version(s): * Up to (including) 8.5.02.005					
Authorization Bypass Through User-Controlled Key	19-Dec-2023	7.5	Authorization Bypass Through User-Controlled Key vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus.This issue affects WP Photo Album Plus: from n/a through 8.5.02.005.	N/A	A-WPP-WP_P-160124/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-49812		
Vendor: wpvibes					
Product: redirect_404_error_page_to_homepage_or_custom_page_with_logs					
Affected Version(s): * Up to (excluding) 1.8.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Dec-2023	7.2	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPVibes Redirect 404 Error Page to Homepage or Custom Page with Logs allows SQL Injection.This issue affects Redirect 404 Error Page to Homepage or Custom Page with Logs: from n/a through 1.8.7. **CVE ID : CVE-2023-47530**	N/A	A-WPV-REDI-160124/686
Vendor: wpvnteam					
Product: wp_extra					
Affected Version(s): * Up to (including) 6.2					
Cross-Site Request Forgery (CSRF)	19-Dec-2023	8.8	Missing Authorization, Cross-Site Request Forgery (CSRF) vulnerability in TienCOP WP EXtra allows Accessing Functionality Not Properly	N/A	A-WPV-WP_E-160124/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Constrained by ACLs, Cross Site Request Forgery.This issue affects WP EXtra: from n/a through 6.2. **CVE ID : CVE-2023-46212**		
Vendor: Wso2					
Product: api_manager					
Affected Version(s): 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/688
Affected Version(s): 2.5.0					
Improper Neutralization of Input During Web Page Generation	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/202	A-WSO-API_-160124/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			(XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	1/WSO2-2020-1225/	
Affected Version(s): 2.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/690
Affected Version(s): 3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**		
Affected Version(s): 3.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/692
Affected Version(s): 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Console. **CVE ID : CVE-2023-6911**		
Product: api_manager_analytics					
Affected Version(s): 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/694
Affected Version(s): 2.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console.	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6911		
Product: api_microgateway					
Affected Version(s): 2.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-API_-160124/696
Product: data_analytics_server					
Affected Version(s): 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console.	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-DATA-160124/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6911		
Product: enterprise_integrator					
Affected Version(s): 6.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-ENTE-160124/698
Affected Version(s): 6.1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console.	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-ENTE-160124/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6911		
Affected Version(s): 6.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-ENTE-160124/700
Affected Version(s): 6.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-ENTE-160124/701
Affected Version(s): 6.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-ENTE-160124/702
Affected Version(s): 6.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-ENTE-160124/703
Affected Version(s): 6.6.0					
Improper Neutralization of	18-Dec-2023	4.8	Multiple WSO2 products have been identified as	https://security.docs.wso2.com/en/latest/secu	A-WSO-ENTE-160124/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	rity-announcements/security-advisories/2021/WSO2-2020-1225/	
Product: identity_server					
Affected Version(s): 5.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/705
Affected Version(s): 5.4.0					
Improper Neutralization of Input During	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output	https://security.docs.wso2.com/en/latest/security-announcements	A-WSO-IDEN-160124/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	/security-advisories/2021/WSO2-2020-1225/	
Affected Version(s): 5.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/707
Affected Version(s): 5.5.0					
Improper Neutralization of Input During Web Page Generation	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/202	A-WSO-IDEN-160124/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	1/WSO2-2020-1225/	
Affected Version(s): 5.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/709
Affected Version(s): 5.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**		
Affected Version(s): 5.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/711
Affected Version(s): 5.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Management Console. **CVE ID : CVE-2023-6911**		
Product: identity_server_analytics					
Affected Version(s): 5.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/713
Affected Version(s): 5.4.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console.	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6911		
Affected Version(s): 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/715
Affected Version(s): 5.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: identity_server_as_key_manager					
Affected Version(s): 5.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/717
Affected Version(s): 5.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/718
Affected Version(s): 5.6.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/719
Affected Version(s): 5.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-IDEN-160124/720
Affected Version(s): 5.9.0					
Improper Neutralization of	18-Dec-2023	4.8	Multiple WSO2 products have been identified as	https://security.docs.wso2.com/en/latest/secu	A-WSO-IDEN-160124/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	rity-announcements/security-advisories/2021/WSO2-2020-1225/	
Product: message_broker					
Affected Version(s): 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2023	4.8	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console. **CVE ID : CVE-2023-6911**	https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2021/WSO2-2020-1225/	A-WSO-MESS-160124/722
Vendor: Xnau					
Product: participants_database					
Affected Version(s): * Up to (including) 2.5.5					
Cross-Site Request	19-Dec-2023	8.8	Missing Authorization,	N/A	A-XNA-PART-160124/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Cross-Site Request Forgery (CSRF) vulnerability in Roland Barker, xnau webdesign Participants Database allows Accessing Functionality Not Properly Constrained by ACLs, Cross Site Request Forgery.This issue affects Participants Database: from n/a through 2.5.5. **CVE ID : CVE-2023-48751**		
Vendor: xtemos					
Product: woodmart					
Affected Version(s): * Up to (excluding) 1.0.37					
Deserialization of Untrusted Data	21-Dec-2023	9.8	Deserialization of Untrusted Data vulnerability in xtemos WoodMart - Multipurpose WooCommerce Theme.This issue affects WoodMart - Multipurpose WooCommerce Theme: from n/a through 1.0.36. **CVE ID : CVE-2023-32242**	N/A	A-XTE-WOOD-160124/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Zabbix					
Product: frontend					
Affected Version(s): 7.0.0					
Reliance on Cookies without Validation and Integrity Checking	18-Dec-2023	8.8	The website configured in the URL widget will receive a session cookie when testing or executing scheduled reports. The received session cookie can then be used to access the frontend as the particular user. **CVE ID : CVE-2023-32725**	https://support.zabbix.com/browse/ZBX-23854	A-ZAB-FRON-160124/725
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.21					
Reliance on Cookies without Validation and Integrity Checking	18-Dec-2023	8.8	The website configured in the URL widget will receive a session cookie when testing or executing scheduled reports. The received session cookie can then be used to access the frontend as the particular user. **CVE ID : CVE-2023-32725**	https://support.zabbix.com/browse/ZBX-23854	A-ZAB-FRON-160124/726
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.6					
Reliance on Cookies without Validation	18-Dec-2023	8.8	The website configured in the URL widget will receive a session	https://support.zabbix.com/browse/ZBX-23854	A-ZAB-FRON-160124/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
and Integrity Checking			cookie when testing or executing scheduled reports. The received session cookie can then be used to access the frontend as the particular user. **CVE ID : CVE-2023-32725**		
Product: zabbix-agent					
Affected Version(s): 7.0.0					
Improper Check for Unusual or Exceptional Conditions	18-Dec-2023	8.1	The vulnerability is caused by improper check for check if RDLENGTH does not overflow the buffer in response from DNS server. **CVE ID : CVE-2023-32726**	https://support.zabbix.com/browse/ZBX-23855	A-ZAB-ZABB-160124/728
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.39					
Improper Check for Unusual or Exceptional Conditions	18-Dec-2023	8.1	The vulnerability is caused by improper check for check if RDLENGTH does not overflow the buffer in response from DNS server. **CVE ID : CVE-2023-32726**	https://support.zabbix.com/browse/ZBX-23855	A-ZAB-ZABB-160124/729
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.23					
Improper Check for Unusual or Exceptiona	18-Dec-2023	8.1	The vulnerability is caused by improper check for check if RDLENGTH does	https://support.zabbix.com/browse/ZBX-23855	A-ZAB-ZABB-160124/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
l Conditions			not overflow the buffer in response from DNS server. **CVE ID : CVE-2023-32726**		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.8					
Improper Check for Unusual or Exceptiona l Conditions	18-Dec-2023	8.1	The vulnerability is caused by improper check for check if RDLENGTH does not overflow the buffer in response from DNS server. **CVE ID : CVE-2023-32726**	https://support.zabbix.com/browse/ZBX-23855	A-ZAB-ZABB-160124/731
Product: zabbix-agent2					
Affected Version(s): 7.0.0					
Improper Control of Generation of Code ('Code Injection')	18-Dec-2023	9.8	The Zabbix Agent 2 item key smart.disk.get does not sanitize its parameters before passing them to a shell command resulting possible vulnerability for remote code execution. **CVE ID : CVE-2023-32728**	https://support.zabbix.com/browse/ZBX-23858	A-ZAB-ZABB-160124/732
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.23					
Improper Control of Generation of Code ('Code Injection')	18-Dec-2023	9.8	The Zabbix Agent 2 item key smart.disk.get does not sanitize its parameters before passing them to a shell command resulting possible vulnerability for	https://support.zabbix.com/browse/ZBX-23858	A-ZAB-ZABB-160124/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. **CVE ID : CVE-2023-32728**		
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.8					
Improper Control of Generation of Code ('Code Injection')	18-Dec-2023	9.8	The Zabbix Agent 2 item key smart.disk.get does not sanitize its parameters before passing them to a shell command resulting possible vulnerability for remote code execution. **CVE ID : CVE-2023-32728**	https://support.zabbix.com/browse/ZBX-23858	A-ZAB-ZABB-160124/734
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.38					
Improper Control of Generation of Code ('Code Injection')	18-Dec-2023	9.8	The Zabbix Agent 2 item key smart.disk.get does not sanitize its parameters before passing them to a shell command resulting possible vulnerability for remote code execution. **CVE ID : CVE-2023-32728**	https://support.zabbix.com/browse/ZBX-23858	A-ZAB-ZABB-160124/735
Product: zabbix_server					
Affected Version(s): 7.0.0					
Reliance on Cookies without Validation and	18-Dec-2023	8.8	The website configured in the URL widget will receive a session cookie when testing or executing	https://support.zabbix.com/browse/ZBX-23854	A-ZAB-ZABB-160124/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integrity Checking			scheduled reports. The received session cookie can then be used to access the frontend as the particular user. **CVE ID : CVE-2023-32725**		
Improper Input Validation	18-Dec-2023	7.2	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious command inside it to execute arbitrary code on the current Zabbix server. **CVE ID : CVE-2023-32727**	https://support.zabbix.com/browse/ZBX-23857	A-ZAB-ZABB-160124/737
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.21					
Reliance on Cookies without Validation and Integrity Checking	18-Dec-2023	8.8	The website configured in the URL widget will receive a session cookie when testing or executing scheduled reports. The received session cookie can then be used to access the frontend as the particular user. **CVE ID : CVE-2023-32725**	https://support.zabbix.com/browse/ZBX-23854	A-ZAB-ZABB-160124/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.6					
Reliance on Cookies without Validation and Integrity Checking	18-Dec-2023	8.8	The website configured in the URL widget will receive a session cookie when testing or executing scheduled reports. The received session cookie can then be used to access the frontend as the particular user. **CVE ID : CVE-2023-32725**	https://support.zabbix.com/browse/ZBX-23854	A-ZAB-ZABB-160124/739
Affected Version(s): From (including) 5.0.0 Up to (including) 5.0.38					
Improper Input Validation	18-Dec-2023	7.2	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious command inside it to execute arbitrary code on the current Zabbix server. **CVE ID : CVE-2023-32727**	https://support.zabbix.com/browse/ZBX-23857	A-ZAB-ZABB-160124/740
Affected Version(s): From (including) 4.0.0 Up to (including) 4.0.49					
Improper Input Validation	18-Dec-2023	7.2	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious	https://support.zabbix.com/browse/ZBX-23857	A-ZAB-ZABB-160124/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command inside it to execute arbitrary code on the current Zabbix server. **CVE ID : CVE-2023-32727**		
Affected Version(s): From (including) 6.0.0 Up to (including) 6.0.22					
Improper Input Validation	18-Dec-2023	7.2	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious command inside it to execute arbitrary code on the current Zabbix server. **CVE ID : CVE-2023-32727**	https://support.zabbix.com/browse/ZBX-23857	A-ZAB-ZABB-160124/742
Affected Version(s): From (including) 6.4.0 Up to (including) 6.4.7					
Improper Input Validation	18-Dec-2023	7.2	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious command inside it to execute arbitrary code on the current Zabbix server. **CVE ID : CVE-2023-32727**	https://support.zabbix.com/browse/ZBX-23857	A-ZAB-ZABB-160124/743
Vendor: zackgrossbart					
Product: editorial_calendar					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 3.8.0					
Authorization Bypass Through User-Controlled Key	20-Dec-2023	8.1	Authorization Bypass Through User-Controlled Key vulnerability in MarketingFire Editorial Calendar.This issue affects Editorial Calendar: from n/a through 3.7.12. **CVE ID : CVE-2023-36520**	N/A	A-ZAC-EDIT-160124/744
Vendor: zendrop					
Product: zendrop					
Affected Version(s): * Up to (excluding) 1.0.1					
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in Zendrop Zendrop – Global Dropshipping.This issue affects Zendrop – Global Dropshipping: from n/a through 1.0.0. **CVE ID : CVE-2023-25970**	N/A	A-ZEN-ZEND-160124/745
Hardware					
Vendor: bosch					
Product: cpp13					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Dec-2023	7.2	A command injection vulnerability exists in Bosch IP cameras that allows an authenticated user with administrative rights to run arbitrary commands on the OS of the camera. **CVE ID : CVE-2023-39509**	https://psirt.bosch.com/security-advisories/BOSCH-SA-638184-BT.html	H-BOS-CPP1-170124/746
Product: cpp14					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Dec-2023	7.2	A command injection vulnerability exists in Bosch IP cameras that allows an authenticated user with administrative rights to run arbitrary commands on the OS of the camera. **CVE ID : CVE-2023-39509**	https://psirt.bosch.com/security-advisories/BOSCH-SA-638184-BT.html	H-BOS-CPP1-170124/747
Product: divar_ip_7000_r2					
Affected Version(s): -					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	H-BOS-DIVA-170124/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**		
Product: divar_ip_all-in-one_4000					
Affected Version(s): -					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	H-BOS-DIVA-170124/749
Product: divar_ip_all-in-one_5000					
Affected Version(s): -					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to	https://psirt.bosch.com/security-advisories/BOS	H-BOS-DIVA-170124/750

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	CH-SA-092656-BT.html	
Product: divar_ip_all-in-one_6000					
Affected Version(s): -					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	H-BOS-DIVA-170124/751
Product: divar_ip_all-in-one_7000					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	H-BOS-DIVA-170124/752
Product: divar_ip_all-in-one_7000_r3					
Affected Version(s): -					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	H-BOS-DIVA-170124/753

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: videojet_decoder_7513					
Affected Version(s): -					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	H-BOS-VIDE-170124/754
Product: videojet_decoder_7523					
Affected Version(s): -					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	H-BOS-VIDE-170124/755
Vendor: cambiumnetworks					
Product: epmp_force_300-25					
Affected Version(s): -					
Improper Control of Generation of Code ('Code Injection')	18-Dec-2023	7.8	Cambium ePMP Force 300-25 version 4.7.0.1 is vulnerable to a code injection vulnerability that	N/A	H-CAM-EPMP-170124/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker to perform remote code execution and gain root privileges. **CVE ID : CVE-2023-6691**		
Vendor: Dlink					
Product: dir-850l					
Affected Version(s): b1					
Improper Control of Generation of Code ('Code Injection')	19-Dec-2023	9.8	An issue in D-Link DIR-850L v.B1_FW223WWb01 allows a remote attacker to execute arbitrary code via a crafted script to the en parameter. **CVE ID : CVE-2023-49004**	N/A	H-DLI-DIR--170124/757
Vendor: efacec					
Product: bcu_500					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	20-Dec-2023	8.8	A successful CSRF attack could force the user to perform state changing	N/A	H-EFA-BCU_-170124/758

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests on the application. If the victim is an administrative account, a CSRF attack could compromise the entire web application. **CVE ID : CVE-2023-6689**		
Uncontrolled Resource Consumption	20-Dec-2023	7.5	Through the exploitation of active user sessions, an attacker could send custom requests to cause a denial-of-service condition on the device. **CVE ID : CVE-2023-50707**	N/A	H-EFA-BCU_-170124/759
Product: uc_500e					
Affected Version(s): -					
URL Redirection to Untrusted	20-Dec-2023	6.1		N/A	H-EFA-UC_5-170124/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			An attacker could construct a URL within the application that causes a redirection to an arbitrary external domain and could be leveraged to facilitate phishing attacks against application users. **CVE ID : CVE-2023-50704**		
Cleartext Transmission of Sensitive Information	20-Dec-2023	5.9	An attacker with network access could perform a man-in-the-middle (MitM) attack and capture sensitive information to gain unauthorized access to the application.	N/A	H-EFA-UC_5-170124/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50703		
Incorrect Authorization	20-Dec-2023	5.3	An attacker could create malicious requests to obtain sensitive information about the web server. **CVE ID : CVE-2023-50705**	N/A	H-EFA-UC_5-170124/762
N/A	20-Dec-2023	4.3		N/A	H-EFA-UC_5-170124/763

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A user without administrator permissions with access to the UC500 windows system could perform a memory dump of the running processes and extract clear credentials or valid session tokens. **CVE ID : CVE-2023-50706**		
Vendor: eurotel					
Product: etl3100					
Affected Version(s): -					
Improper Restriction of Excessive Authentication Attempts	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 does not limit the number of attempts to guess administrative credentials in remote password attacks to gain full	N/A	H-EUR-ETL3-170124/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			control of the system. **CVE ID : CVE-2023-6928**		
Authorization Bypass Through User-Controlled Key	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 are vulnerable to insecure direct object references that occur when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability, attackers can bypass authorization, access the hidden resources on the system, and execute privileged functionalities.	N/A	H-EUR-ETL3-170124/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6929		
N/A	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 suffer from an unauthenticated configuration and log download vulnerability. This enables the attacker to disclose sensitive information and assist in authentication bypass, privilege escalation, and full system access.	N/A	H-EUR-ETL3-170124/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6930		
Vendor: gallagher					
Product: controller_6000					
Affected Version(s): -					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	H-GAL-CONT-170124/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Product: controller_7000					
Affected Version(s): -					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diagnostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)),	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	H-GAL-CONT-170124/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Vendor: Hikvision					
Product: ds-kd-bk					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\	N/A	H-HIK-DS-K-170124/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is	N/A	H-HIK-DS-K-170124/770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd-dis					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is	N/A	H-HIK-DS-K-170124/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was	N/A	H-HIK-DS-K-170124/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd-e					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this	N/A	H-HIK-DS-K-170124/773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**	N/A	H-HIK-DS-K-170124/774
Product: ds-kd-in					
Affected Version(s): -					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**	N/A	H-HIK-DS-K-170124/775
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom	N/A	H-HIK-DS-K-170124/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd-info					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as	N/A	H-HIK-DS-K-170124/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of	N/A	H-HIK-DS-K-170124/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd-kk					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The	N/A	H-HIK-DS-K-170124/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The	N/A	H-HIK-DS-K-170124/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd-kk\/s					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The	N/A	H-HIK-DS-K-170124/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to	N/A	H-HIK-DS-K-170124/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd-kp					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to	N/A	H-HIK-DS-K-170124/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability.	N/A	H-HIK-DS-K-170124/784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6894		
Product: ds-kd-kp\/s					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252.	N/A	H-HIK-DS-K-170124/785

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6893		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**	N/A	H-HIK-DS-K-170124/786
Product: ds-kd-m					
Affected Version(s): -					
Improper Limitation	17-Dec-2023	7.5	A vulnerability was found in Hikvision	N/A	H-HIK-DS-K-170124/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System	N/A	H-HIK-DS-K-170124/788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd3003-e6					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this	N/A	H-HIK-DS-K-170124/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/syste	N/A	H-HIK-DS-K-170124/790

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			m.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd8003ime1\(b\)					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument	N/A	H-HIK-DS-K-170124/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the	N/A	H-HIK-DS-K-170124/792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd8003ime1\(b\)\/flush					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the	N/A	H-HIK-DS-K-170124/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component	N/A	H-HIK-DS-K-170124/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kd8003ime1\(b\)\/ns					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected	N/A	H-HIK-DS-K-170124/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**	N/A	H-HIK-DS-K-170124/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ds-kd8003ime1\(b\)\/s					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**	N/A	H-HIK-DS-K-170124/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**	N/A	H-HIK-DS-K-170124/798
Product: ds-kd8003ime1\(b\)\/surface					
Affected Version(s): -					
Improper Limitation of a Pathname to a	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System	N/A	H-HIK-DS-K-170124/799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified	N/A	H-HIK-DS-K-170124/800

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6220-le1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the	N/A	H-HIK-DS-K-170124/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The	N/A	H-HIK-DS-K-170124/802

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6320-le1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\	N/A	H-HIK-DS-K-170124/803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is	N/A	H-HIK-DS-K-170124/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6320-tde1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is	N/A	H-HIK-DS-K-170124/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was	N/A	H-HIK-DS-K-170124/806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6320-te1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this	N/A	H-HIK-DS-K-170124/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**	N/A	H-HIK-DS-K-170124/808
Product: ds-kh6320-wtde1					
Affected Version(s): -					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**	N/A	H-HIK-DS-K-170124/809
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom	N/A	H-HIK-DS-K-170124/810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6320-wte1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as	N/A	H-HIK-DS-K-170124/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of	N/A	H-HIK-DS-K-170124/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6350-wte1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The	N/A	H-HIK-DS-K-170124/813

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The	N/A	H-HIK-DS-K-170124/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6351-te1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The	N/A	H-HIK-DS-K-170124/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to	N/A	H-HIK-DS-K-170124/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh6351-wte1					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to	N/A	H-HIK-DS-K-170124/817

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability.	N/A	H-HIK-DS-K-170124/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6894		
Product: ds-kh63le1\(b\)					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252.	N/A	H-HIK-DS-K-170124/819

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6893		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**	N/A	H-HIK-DS-K-170124/820
Product: ds-kh8520-wte1					
Affected Version(s): -					
Improper Limitation	17-Dec-2023	7.5	A vulnerability was found in Hikvision	N/A	H-HIK-DS-K-170124/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System	N/A	H-HIK-DS-K-170124/822

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh9310-wte1\(b\)					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this	N/A	H-HIK-DS-K-170124/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/syste	N/A	H-HIK-DS-K-170124/824

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			m.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Product: ds-kh9510-wte1\(b\)					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument	N/A	H-HIK-DS-K-170124/825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the	N/A	H-HIK-DS-K-170124/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Vendor: hitachienergy					
Product: rtu500					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&languageCode=en&Preview=true	H-HIT-RTU5-170124/827
Vendor: hpe					
Product: integrated_lights-out_5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	19-Dec-2023	9.8	A potential security vulnerability has been identified in HPE Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 6 (iLO 6). The vulnerability could be remotely exploited to allow authentication bypass. **CVE ID : CVE-2023-50272**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04584en_us	H-HPE-INTE-170124/828
Product: integrated_lights-out_6					
Affected Version(s): -					
N/A	19-Dec-2023	9.8	A potential security vulnerability has been identified in HPE Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 6 (iLO 6). The vulnerability could be remotely exploited to allow authentication bypass. **CVE ID : CVE-2023-50272**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04584en_us	H-HPE-INTE-170124/829
Vendor: Moxa					
Product: iologik_e1210					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in	https://www.moxa.com/en/support/product-support/security-	H-MOX-IOLO-170124/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	
Product: iologik_e1211					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**		
Product: iologik_e1212					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: iologik_e1213					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/833
Product: iologik_e1214					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-	H-MOX-IOLO-170124/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	web-server-vulnerability	
Product: iologik_e1240					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**		
Product: iologik_e1241					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/836
Product: iologik_e1242					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/837
Product: iologik_e1260					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**		
Product: iologik_e1262					
Affected Version(s): -					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user.	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	H-MOX-IOLO-170124/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5961		
Vendor: ruijie					
Product: rg-ws6008					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Dec-2023	9.8	Ruijie WS6008 v1.x v2.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 and WS6108 v1.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 was discovered to contain a command injection vulnerability via the function downFiles. **CVE ID : CVE-2023-50993**	N/A	H-RUI-RG-W-170124/840
Affected Version(s): 2.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Dec-2023	9.8	Ruijie WS6008 v1.x v2.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 and WS6108 v1.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 was discovered to contain a command injection vulnerability via the function downFiles.	N/A	H-RUI-RG-W-170124/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50993		
Product: rg-ws6108					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Dec-2023	9.8	Ruijie WS6008 v1.x v2.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 and WS6108 v1.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 was discovered to contain a command injection vulnerability via the function downFiles. **CVE ID : CVE-2023-50993**	N/A	H-RUI-RG-W-170124/842
Vendor: Tenda					
Product: i29					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a command injection vulnerability via the sysScheduleRebootSet function. **CVE ID : CVE-2023-50983**	N/A	H-TEN-I29-170124/843
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the ip parameter in the	N/A	H-TEN-I29-170124/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spdtstConfigAndStart function. **CVE ID : CVE-2023-50984**		
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the lanGw parameter in the lanCfgSet function. **CVE ID : CVE-2023-50985**	N/A	H-TEN-I29-170124/845
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the time parameter in the sysLogin function. **CVE ID : CVE-2023-50986**	N/A	H-TEN-I29-170124/846
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the time parameter in the sysTimeInfoSet function. **CVE ID : CVE-2023-50987**	N/A	H-TEN-I29-170124/847
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the bandwidth parameter in the	N/A	H-TEN-I29-170124/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wifiRadioSetIndoor function. **CVE ID : CVE-2023-50988**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a command injection vulnerability via the pingSet function. **CVE ID : CVE-2023-50989**	N/A	H-TEN-I29-170124/849
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the rebootTime parameter in the sysScheduleRebootSet function. **CVE ID : CVE-2023-50990**	N/A	H-TEN-I29-170124/850
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a stack overflow via the ip parameter in the setPing function. **CVE ID : CVE-2023-50992**	N/A	H-TEN-I29-170124/851
Product: m3					
Affected Version(s): -					
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the	N/A	H-TEN-M3-170124/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function formGetWeiXinConfig. **CVE ID : CVE-2023-51090**		
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function R7WebsSecurityHandler. **CVE ID : CVE-2023-51091**	N/A	H-TEN-M3-170124/853
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function upgrade. **CVE ID : CVE-2023-51092**	N/A	H-TEN-M3-170124/854
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function fromSetLocalVlanInfo. **CVE ID : CVE-2023-51093**	N/A	H-TEN-M3-170124/855
Improper Neutralization of Special Elements used in an OS Command	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a Command Execution vulnerability via	N/A	H-TEN-M3-170124/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			the function TendaTelnet. **CVE ID : CVE-2023-51094**		
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function formDelWlRfPolicy . **CVE ID : CVE-2023-51095**	N/A	H-TEN-M3-170124/857
Product: w9					
Affected Version(s): -					
Out-of-bounds Write	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a stack overflow via the function formSetAutoPing. **CVE ID : CVE-2023-51097**	N/A	H-TEN-W9-170124/858
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a command injection vulnerability via the function formSetDiagnoseInfo . **CVE ID : CVE-2023-51098**	N/A	H-TEN-W9-170124/859
Improper Neutralization of Special Elements	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a command injection	N/A	H-TEN-W9-170124/860

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			vulnerability via the function formexeCommand . **CVE ID : CVE-2023-51099**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a command injection vulnerability via the function formGetDiagnoseInfo . **CVE ID : CVE-2023-51100**	N/A	H-TEN-W9-170124/861
Out-of-bounds Write	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a stack overflow via the function formSetUplinkInfo. **CVE ID : CVE-2023-51101**	N/A	H-TEN-W9-170124/862
Out-of-bounds Write	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a stack overflow via the function formWifiMacFilterSet. **CVE ID : CVE-2023-51102**	N/A	H-TEN-W9-170124/863
Vendor: totolink					
Product: a3700r					
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')	22-Dec-2023	9.8	There is an arbitrary command execution vulnerability in the setDiagnosisCfg function of the cstecgi .cgi of the TOTOlink A3700R router device in its firmware version V9.1.2u.5822_B20200513. **CVE ID : CVE-2023-50147**	N/A	H-TOT-A370-170124/864
Product: a7100ru					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Dec-2023	9.8	A vulnerability, which was classified as critical, was found in Totolink A7100RU 7.4cu.2313_B20191024. Affected is the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument flag with the input ie8 leads to buffer overflow. 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	N/A	H-TOT-A710-170124/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is VDB-248268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6906**		
Product: ex1200l					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Dec-2023	9.8	TOTOlink EX1200L V9.3.5u.6146_B20201023 is vulnerable to arbitrary command execution via the cstecgi.cgi setOpModeCfg interface. **CVE ID : CVE-2023-51033**	N/A	H-TOT-EX12-170124/866
Product: ex1800t					
Affected Version(s): -					
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the lanPriDns parameter' of the setLanConfig interface of the cstecgi .cgi **CVE ID : CVE-2023-51011**	N/A	H-TOT-EX18-170124/867
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is	N/A	H-TOT-EX18-170124/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to unauthorized arbitrary command execution in the lanGateway parameter' of the setLanConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51012**		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the lanNetmask parameter' of the setLanConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51013**	N/A	H-TOT-EX18-170124/869
N/A	22-Dec-2023	9.8	TOTOLINK EX1800T V9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the lanSecDns parameter' of the setLanConfig interface of the cstecgi .cgi **CVE ID : CVE-2023-51014**	N/A	H-TOT-EX18-170124/870
N/A	22-Dec-2023	9.8	TOTOLINX EX1800T	N/A	H-TOT-EX18-170124/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v9.1.0cu.2112_B20 220316 is vulnerable to arbitrary command execution in the 'enable parameter' of the setDmzCfg interface of the cstecgi .cgi **CVE ID : CVE-2023-51015**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the setRebootScheCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51016**	N/A	H-TOT-EX18-170124/872
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the lanIp parameter' of the setLanConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51017**	N/A	H-TOT-EX18-170124/873
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command	N/A	H-TOT-EX18-170124/874

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the 'opmode' parameter of the setWiFiApConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51018**		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'key5g' parameter of the setWiFiExtenderConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51019**	N/A	H-TOT-EX18-170124/875
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'langType' parameter of the setLanguageCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51020**	N/A	H-TOT-EX18-170124/876
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command	N/A	H-TOT-EX18-170124/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution in the 'merge' parameter of the setRptWizardCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51021**		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'langFlag' parameter of the setLanguageCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51022**	N/A	H-TOT-EX18-170124/878
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to arbitrary command execution in the 'host_time' parameter of the NTPSyncWithHost interface of the cstecgi .cgi. **CVE ID : CVE-2023-51023**	N/A	H-TOT-EX18-170124/879
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'tz'	N/A	H-TOT-EX18-170124/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter of the setNtpCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51024**		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T V9.1.0cu.2112_B20220316 is vulnerable to an unauthorized arbitrary command execution in the 'admuser' parameter of the setPasswordCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51025**	N/A	H-TOT-EX18-170124/881
N/A	22-Dec-2023	9.8	TOTOlink EX1800T V9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'hour' parameter of the setRebootScheCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51026**	N/A	H-TOT-EX18-170124/882
N/A	22-Dec-2023	9.8	TOTOlink EX1800T V9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'apcliAuthMode' parameter of the	N/A	H-TOT-EX18-170124/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			setWiFiExtenderConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51027**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Dec-2023	9.8	TOTOLINK EX1800T 9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the apcliChannel parameter of the setWiFiExtenderConfig interface of the cstecgi.cgi. **CVE ID : CVE-2023-51028**	N/A	H-TOT-EX18-170124/884
Vendor: weintek					
Product: cmt2078x					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2023	8.8	An authenticated command injection vulnerability in Weintek cMT2078X easyweb Web Version v2.1.3, OS v20220215 allows attackers to execute arbitrary code or access sensitive information via injecting a crafted payload into the HMI Name parameter.	N/A	H-WEI-CMT2-170124/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-50466		
Operating System					
Vendor: Apple					
Product: macos					
Affected Version(s): -					
Missing Authentication for Critical Function	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before on Windows and 2.6.9 and before on macOS, allows attackers to bypass network filtering, execute arbitrary code, and obtain sensitive information via DarkLayer Guard threat prevention module. **CVE ID : CVE-2023-29485**	N/A	O-APP-MACO-170124/886
N/A	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before 3.7.0 on Windows, allows attackers to bypass USB access restrictions, execute arbitrary code, and obtain sensitive information via Next-Gen Antivirus component.	N/A	O-APP-MACO-170124/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-29486		
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-APP-MACO-170124/888

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Concurrent Execution using	19-Dec-2023	5.3	When resolving a symlink, a race may occur where	https://www.mozilla.org/security/advisories/	O-APP-MACO-170124/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**	mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	
Vendor: bosch					
Product: cpp13_firmware					
Affected Version(s): * Up to (including) 8.90					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Dec-2023	7.2	A command injection vulnerability exists in Bosch IP cameras that allows an authenticated user with administrative rights to run arbitrary commands on the OS of the camera. **CVE ID : CVE-2023-39509**	https://psirt.bosch.com/security-advisories/BOSCH-SA-638184-BT.html	O-BOS-CPP1-170124/890
Product: cpp14_firmware					
Affected Version(s): From (including) 8.20 Up to (including) 8.81					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Dec-2023	7.2	A command injection vulnerability exists in Bosch IP cameras that allows an authenticated user with administrative rights to run arbitrary commands on the OS of the camera. **CVE ID : CVE-2023-39509**	https://psirt.bosch.com/security-advisories/BOSCH-SA-638184-BT.html	O-BOS-CPP1-170124/891
Product: divar_ip_7000_r2_firmware					
Affected Version(s): * Up to (including) 12.0					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	O-BOS-DIVA-170124/892
Product: divar_ip_all-in-one_4000_firmware					
Affected Version(s): * Up to (including) 12.0					
N/A	18-Dec-2023	5.9	An improper handling of a	https://psirt.bosch.com/securit	O-BOS-DIVA-170124/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	y-advisories/BOSCH-SA-092656-BT.html	
Product: divar_ip_all-in-one_5000_firmware					
Affected Version(s): * Up to (including) 12.0					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	O-BOS-DIVA-170124/894
Product: divar_ip_all-in-one_6000_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 12.0					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	O-BOS-DIVA-170124/895
Product: divar_ip_all-in-one_7000_firmware					
Affected Version(s): * Up to (including) 12.0					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks.	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	O-BOS-DIVA-170124/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-35867		
Product: divar_ip_all-in-one_7000_r3_firmware					
Affected Version(s): * Up to (including) 12.0					
N/A	18-Dec-2023	5.9	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks. **CVE ID : CVE-2023-35867**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	O-BOS-DIVA-170124/897
Product: videojet_decoder_7513_firmware					
Affected Version(s): * Up to (including) 10.40.0055					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	O-BOS-VIDE-170124/898
Product: videojet_decoder_7523_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 10.40.0055					
N/A	18-Dec-2023	7.5	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. **CVE ID : CVE-2023-32230**	https://psirt.bosch.com/security-advisories/BOSCH-SA-092656-BT.html	O-BOS-VIDE-170124/899
Vendor: cambiumnetworks					
Product: epmp_force_300-25_firmware					
Affected Version(s): 4.7.0.1					
Improper Control of Generation of Code ('Code Injection')	18-Dec-2023	7.8	Cambium ePMP Force 300-25 version 4.7.0.1 is vulnerable to a code injection vulnerability that could allow an attacker to perform remote code execution and gain root privileges. **CVE ID : CVE-2023-6691**	N/A	O-CAM-EPMP-170124/900
Vendor: Debian					
Product: debian_linux					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-DEB-DEBI-170124/901

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Affected Version(s): 10.0					
Improper Limitation of a	18-Dec-2023	6.3	An absolute path traversal attack exists in the	https://access.redhat.com/errata/RHSA-	O-DEB-DEBI-170124/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	
Affected Version(s): 11.0					
Out-of-bounds Write	19-Dec-2023	8.8	The WebGL `DrawElementsInstanced` method was susceptible to a heap buffer overflow when used on systems with the Mesa VM driver. This issue could allow an attacker to perform remote code execution and sandbox escape. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6856**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/903
Out-of-bounds Write	19-Dec-2023	8.8	Firefox was susceptible to a heap buffer overflow in `nsTextFragment` due to insufficient	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/secur	O-DEB-DEBI-170124/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			OOM handling. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6858**	ity/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	
Use After Free	19-Dec-2023	8.8	A use-after-free condition affected TLS socket creation when under memory pressure. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6859**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/905
Out-of-bounds Write	19-Dec-2023	8.8	The `nsWindow::PickerOpen(void)` method was susceptible to a heap buffer overflow when running in headless mode. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6861**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/906
Use After Free	19-Dec-2023	8.8	A use-after-free was identified in the	https://www.mozilla.org/security/advisories/	O-DEB-DEBI-170124/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`nsDNSService::Init`. This issue appears to manifest rarely during start-up. This vulnerability affects Firefox ESR < 115.6 and Thunderbird < 115.6. **CVE ID : CVE-2023-6862**	mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/	
N/A	19-Dec-2023	8.8	The `ShutdownObserver()` was susceptible to potentially undefined behavior due to its reliance on a dynamic type that lacked a virtual destructor. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6863**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/908
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			run arbitrary code. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6864**		
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6873**	https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/910
Out-of-bounds Write	21-Dec-2023	8.8	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-7024**	https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html	O-DEB-DEBI-170124/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Dec-2023	6.5	The `VideoBridge` allowed any content process to use textures produced by remote decoders. This could be abused to escape the sandbox. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6860**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/912
N/A	19-Dec-2023	6.5	`EncryptingOutputStream` was susceptible to exposing uninitialized data. This issue could only be abused in order to write data to a local disk which may have implications for private browsing mode. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121. **CVE ID : CVE-2023-6865**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/913
Improper Restriction of Rendered UI Layers or Frames	19-Dec-2023	6.1	The timing of a button click causing a popup to disappear was approximately the same length as the anti-clickjacking	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/secur	O-DEB-DEBI-170124/914

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121. **CVE ID : CVE-2023-6867**	ity/advisories/mfsa2023-56/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	5.3	When resolving a symlink, a race may occur where the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/915
N/A	19-Dec-2023	4.3	The signature of a digitally signed S/MIME email	https://www.mozilla.org/secur	O-DEB-DEBI-170124/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message may optionally specify the signature creation date and time. If present, Thunderbird did not compare the signature creation date with the message date and time, and displayed a valid signature despite a date or time mismatch. This could be used to give recipients the impression that a message was sent at a different date or time. This vulnerability affects Thunderbird < 115.6. **CVE ID : CVE-2023-50761**	ity/advisories/mfsa2023-55/	
N/A	19-Dec-2023	4.3	When processing a PGP/MIME payload that contains digitally signed text, the first paragraph of the text was never shown to the user. This is because the text was interpreted as a MIME message and the first paragraph was always treated as an email header section. A digitally signed text from a	https://www.mozilla.org/security/advisories/mfsa2023-55/	O-DEB-DEBI-170124/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			different context, such as a signed GIT commit, could be used to spoof an email message. This vulnerability affects Thunderbird < 115.6. **CVE ID : CVE-2023-50762**		
Affected Version(s): 12.0					
Out-of-bounds Write	19-Dec-2023	8.8	The WebGL `DrawElementsInstanced` method was susceptible to a heap buffer overflow when used on systems with the Mesa VM driver. This issue could allow an attacker to perform remote code execution and sandbox escape. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6856**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/918
Out-of-bounds Write	19-Dec-2023	8.8	Firefox was susceptible to a heap buffer overflow in `nsTextFragment` due to insufficient OOM handling. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/,	O-DEB-DEBI-170124/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6858**	https://www.mozilla.org/security/advisories/mfsa2023-56/	
Use After Free	19-Dec-2023	8.8	A use-after-free condition affected TLS socket creation when under memory pressure. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6859**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/920
Out-of-bounds Write	19-Dec-2023	8.8	The `nsWindow::PickerOpen(void)` method was susceptible to a heap buffer overflow when running in headless mode. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6861**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/921
Use After Free	19-Dec-2023	8.8	A use-after-free was identified in the `nsDNSService::Init`. This issue	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.m	O-DEB-DEBI-170124/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			appears to manifest rarely during start-up. This vulnerability affects Firefox ESR < 115.6 and Thunderbird < 115.6. **CVE ID : CVE-2023-6862**	ozilla.org/security/advisories/mfsa2023-55/	
N/A	19-Dec-2023	8.8	The `ShutdownObserver()` was susceptible to potentially undefined behavior due to its reliance on a dynamic type that lacked a virtual destructor. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6863**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/923
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6864**		
Out-of-bounds Write	19-Dec-2023	8.8	Memory safety bugs present in Firefox 120. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6873**	https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/925
Out-of-bounds Write	21-Dec-2023	8.8	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-7024**	https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html	O-DEB-DEBI-170124/926
N/A	19-Dec-2023	6.5	The `VideoBridge` allowed any content process to	https://www.mozilla.org/security/advisories/	O-DEB-DEBI-170124/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			use textures produced by remote decoders. This could be abused to escape the sandbox. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6860**	mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	
N/A	19-Dec-2023	6.5	`EncryptingOutputStream` was susceptible to exposing uninitialized data. This issue could only be abused in order to write data to a local disk which may have implications for private browsing mode. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121. **CVE ID : CVE-2023-6865**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/928
Improper Restriction of Rendered UI Layers or Frames	19-Dec-2023	6.1	The timing of a button click causing a popup to disappear was approximately the same length as the anti-clickjacking delay on permission prompts. It was	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121. **CVE ID : CVE-2023-6867**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	5.3	When resolving a symlink, a race may occur where the buffer passed to \`readlink\` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-DEB-DEBI-170124/930
N/A	19-Dec-2023	4.3	The signature of a digitally signed S/MIME email message may optionally specify the signature	https://www.mozilla.org/security/advisories/mfsa2023-55/	O-DEB-DEBI-170124/931

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			creation date and time. If present, Thunderbird did not compare the signature creation date with the message date and time, and displayed a valid signature despite a date or time mismatch. This could be used to give recipients the impression that a message was sent at a different date or time. This vulnerability affects Thunderbird < 115.6. **CVE ID : CVE-2023-50761**		
N/A	19-Dec-2023	4.3	When processing a PGP/MIME payload that contains digitally signed text, the first paragraph of the text was never shown to the user. This is because the text was interpreted as a MIME message and the first paragraph was always treated as an email header section. A digitally signed text from a different context, such as a signed GIT commit, could	https://www.mozilla.org/security/advisories/mfsa2023-55/	O-DEB-DEBI-170124/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be used to spoof an email message. This vulnerability affects Thunderbird < 115.6. **CVE ID : CVE-2023-50762**		
Vendor: Dlink					
Product: dir-850l_firmware					
Affected Version(s): fw223wwb01					
Improper Control of Generation of Code ('Code Injection')	19-Dec-2023	9.8	An issue in D-Link DIR-850L v.B1_FW223WWb01 allows a remote attacker to execute arbitrary code via a crafted script to the en parameter. **CVE ID : CVE-2023-49004**	N/A	O-DLI-DIR--170124/933
Vendor: efacec					
Product: bcu_500_firmware					
Affected Version(s): 4.07					
Cross-Site Request Forgery (CSRF)	20-Dec-2023	8.8	A successful CSRF attack could force the user to perform state changing requests on the application. If the victim is an administrative account, a CSRF attack could	N/A	O-EFA-BCU_-170124/934

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			compromise the entire web application. **CVE ID : CVE-2023-6689**		
Uncontrolled Resource Consumption	20-Dec-2023	7.5	Through the exploitation of active user sessions, an attacker could send custom requests to cause a denial-of-service condition on the device. **CVE ID : CVE-2023-50707**	N/A	O-EFA-BCU_-170124/935
Product: uc_500e_firmware					
Affected Version(s): 10.1.0					
URL Redirection to Untrusted Site ('Open Redirect')	20-Dec-2023	6.1	An attacker could construct a URL within the application that	N/A	O-EFA-UC_5-170124/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			causes a redirection to an arbitrary external domain and could be leveraged to facilitate phishing attacks against application users. **CVE ID : CVE-2023-50704**		
Cleartext Transmission of Sensitive Information	20-Dec-2023	5.9	An attacker with network access could perform a man-in-the-middle (MitM) attack and capture sensitive information to gain unauthorized access to the application. **CVE ID : CVE-2023-50703**	N/A	O-EFA-UC_5-170124/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Dec-2023	5.3	An attacker could create malicious requests to obtain sensitive information about the web server. **CVE ID : CVE-2023-50705**	N/A	O-EFA-UC_5-170124/938
N/A	20-Dec-2023	4.3		N/A	O-EFA-UC_5-170124/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A user without administrator permissions with access to the UC500 windows system could perform a memory dump of the running processes and extract clear credentials or valid session tokens. **CVE ID : CVE-2023-50706**		
Vendor: eurotel					
Product: etl3100_firmware					
Affected Version(s): 01c01					
Improper Restriction of Excessive Authentication Attempts	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 does not limit the number of attempts to guess administrative credentials in remote password attacks to gain full control of the system.	N/A	O-EUR-ETL3-170124/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6928		
Authorization Bypass Through User-Controlled Key	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 are vulnerable to insecure direct object references that occur when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability, attackers can bypass authorization, access the hidden resources on the system, and execute privileged functionalities.	N/A	O-EUR-ETL3-170124/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6929		
N/A	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 suffer from an unauthenticated configuration and log download vulnerability. This enables the attacker to disclose sensitive information and assist in authentication bypass, privilege escalation, and full system access.	N/A	O-EUR-ETL3-170124/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6930		
Affected Version(s): 01x37					
Improper Restriction of Excessive Authentication Attempts	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 does not limit the number of attempts to guess administrative credentials in remote password attacks to gain full control of the system. **CVE ID : CVE-2023-6928**	N/A	O-EUR-ETL3-170124/943
Authorization Bypass Through User-Controlled Key	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 are vulnerable to insecure direct object references that occur when	N/A	O-EUR-ETL3-170124/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the application provides direct access to objects based on user-supplied input. As a result of this vulnerability, attackers can bypass authorization, access the hidden resources on the system, and execute privileged functionalities. **CVE ID : CVE-2023-6929**		
N/A	19-Dec-2023	9.8	EuroTel ETL3100 versions v01c01 and v01x37 suffer from an	N/A	O-EUR-ETL3-170124/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated configuration and log download vulnerability. This enables the attacker to disclose sensitive information and assist in authentication bypass, privilege escalation, and full system access. **CVE ID : CVE-2023-6930**		
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 38					
Out-of-bounds Write	21-Dec-2023	8.8	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML	https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html	O-FED-FEDO-170124/946

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. (Chromium security severity: High) **CVE ID : CVE-2023-7024**		
Affected Version(s): 39					
Out-of-bounds Write	21-Dec-2023	8.8	Heap buffer overflow in WebRTC in Google Chrome prior to 120.0.6099.129 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-7024**	https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html	O-FED-FEDO-170124/947
Vendor: Freebsd					
Product: freebsd					
Affected Version(s): * Up to (including) 12.4					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627	O-FRE-FREE-170124/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before	bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: gallagher					
Product: controller_6000_firmware					
Affected Version(s): * Up to (including) 8.50					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface.	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	O-GAL-CONT-170124/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Affected Version(s): From (including) 8.60 Up to (excluding) 8.60.231116a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface.	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	O-GAL-CONT-170124/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Affected Version(s): From (including) 8.70 Up to (excluding) 8.70.231204a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web interface (Port 80) can be used to perform a Denial of Service of the	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	O-GAL-CONT-170124/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Affected Version(s): From (including) 8.80 Up to (excluding) 8.80.231204a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web interface (Port 80) can be used to	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	O-GAL-CONT-170124/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Affected Version(s): From (including) 8.90 Up to (excluding) 8.90.231204a					
Improper Input Validation	18-Dec-2023	4.3	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diag nostic web	https://security.gallagher.com/Security-Advisories/CVE-2023-22439	O-GAL-CONT-170124/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior. **CVE ID : CVE-2023-22439**		
Vendor: Google					
Product: android					
Affected Version(s): -					
Concurrent Execution using Shared Resource	19-Dec-2023	5.3	When resolving a symlink, a race may occur where the buffer passed to `readlink` may	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.m	O-GOO-ANDR-170124/954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**	ozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	
N/A	19-Dec-2023	4.3	In some instances, the user-agent would allow push requests which lacked a valid VAPID even though the push manager subscription defined one. This could allow empty messages to be sent from unauthorized parties. *This bug only affects Firefox on Android.* This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6868**	https://www.mozilla.org/security/advisories/mfsa2023-56/	O-GOO-ANDR-170124/955
N/A	19-Dec-2023	4.3	Applications which spawn a Toast notification in a	https://www.mozilla.org/secur	O-GOO-ANDR-170124/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			background thread may have obscured fullscreen notifications displayed by Firefox. *This issue only affects Android versions of Firefox and Firefox Focus.* This vulnerability affects Firefox < 121. **CVE ID : CVE-2023-6870**	ity/advisories/mfsa2023-56/	
Vendor: Hikvision					
Product: intercom_broadcast_system					
Affected Version(s): From (including) 3.0.3 Up to (excluding) 4.1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Dec-2023	7.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The	N/A	O-HIK-INTE-170124/957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252. **CVE ID : CVE-2023-6893**		
N/A	17-Dec-2023	6.5	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to	N/A	O-HIK-INTE-170124/958

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability. **CVE ID : CVE-2023-6894**		
Vendor: hitachienergy					
Product: rtu500_firmware					
Affected Version(s): 13.5.1.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&languageCode=en&Preview=true	O-HIT-RTU5-170124/959
Affected Version(s): From (including) 12.0.1.0 Up to (excluding) 12.0.15.0					
Buffer Copy without Checking Size of Input ('Classic	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&languageCode=en&Preview=true	O-HIT-RTU5-170124/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**		
Affected Version(s): From (including) 12.2.1.0 Up to (excluding) 12.2.12.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&languageCode=en&Preview=true	O-HIT-RTU5-170124/961
Affected Version(s): From (including) 12.4.1.0 Up to (excluding) 12.4.12.0					
Buffer Copy without Checking Size of	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&la	O-HIT-RTU5-170124/962

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	nguageCode=en&Preview=true	
Affected Version(s): From (including) 12.6.1.0 Up to (excluding) 12.6.10.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&languageCode=en&Preview=true	O-HIT-RTU5-170124/963
Affected Version(s): From (including) 12.7.1.0 Up to (excluding) 12.7.7.0					
Buffer Copy without	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC	https://publisher.hitachienergy.com/preview?	O-HIT-RTU5-170124/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	DocumentId=8DBD000184&languageCode=en&Preview=true	
Affected Version(s): From (including) 13.2.1.0 Up to (excluding) 13.2.7.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&languageCode=en&Preview=true	O-HIT-RTU5-170124/965
Affected Version(s): From (including) 13.4.1.0 Up to (excluding) 13.4.4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Dec-2023	7.5	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU. **CVE ID : CVE-2023-6711**	https://publisher.hitachienergy.com/preview?DocumentId=8DBD000184&languageCode=en&Preview=true	O-HIT-RTU5-170124/966
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
N/A	17-Dec-2023	7.5	A potential security vulnerability has been identified with HP-UX System Management Homepage (SMH). This vulnerability could be exploited locally or remotely to disclose information. **CVE ID : CVE-2023-50271**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04551en_us	O-HP-HP-U-170124/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: hpe					
Product: integrated_lights-out_5_firmware					
Affected Version(s): From (including) 2.63 Up to (including) 3.00					
N/A	19-Dec-2023	9.8	A potential security vulnerability has been identified in HPE Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 6 (iLO 6). The vulnerability could be remotely exploited to allow authentication bypass. **CVE ID : CVE-2023-50272**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04584en_us	O-HPE-INTE-170124/968
Product: integrated_lights-out_6_firmware					
Affected Version(s): From (including) 1.05 Up to (including) 1.55					
N/A	19-Dec-2023	9.8	A potential security vulnerability has been identified in HPE Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 6 (iLO 6). The vulnerability could be remotely exploited to allow authentication bypass. **CVE ID : CVE-2023-50272**	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04584en_us	O-HPE-INTE-170124/969
Vendor: IBM					
Product: aix					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2023	9.1	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view modify files on the system. IBM X-Force ID: 271196. **CVE ID : CVE-2023-47702**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271196	O-IBM-AIX-170124/970
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to upload files of a dangerous file type. IBM X-Force ID: 271341. **CVE ID : CVE-2023-47706**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271341	O-IBM-AIX-170124/971
Use of Hard-coded Credentials	20-Dec-2023	7.5	IBM Security Guardium Key Lifecycle Manager 4.3 contains plain text hard-coded credentials or other secrets in source code repository. IBM X-Force ID: 271220. **CVE ID : CVE-2023-47704**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271220	O-IBM-AIX-170124/972

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	IBM Security Guardium Key Lifecycle Manager 4.3 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: 271522. **CVE ID : CVE-2023-47707**	https://www.ibm.com/support/pages/node/7091157	O-IBM-AIX-170124/973
Generation of Error Message Containing Sensitive Information	20-Dec-2023	5.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 271197. **CVE ID : CVE-2023-47703**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271197	O-IBM-AIX-170124/974
Improper Input Validation	20-Dec-2023	4.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an	https://www.ibm.com/support/pages/node/7091157,	O-IBM-AIX-170124/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to manipulate username data due to improper input validation. IBM X-Force ID: 271228. **CVE ID : CVE-2023-47705**	https://exchange.xforce.ibmcloud.com/vulnerabilities/271228	
Affected Version(s): 7.2					
N/A	22-Dec-2023	5.5	IBM AIX 7.2 and 7.3 could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of service. IBM X-Force ID: 267963. **CVE ID : CVE-2023-45165**	https://www.ibm.com/support/pages/node/7100970, https://exchange.xforce.ibmcloud.com/vulnerabilities/267963	O-IBM-AIX-170124/976
N/A	19-Dec-2023	5.5	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in AIX windows to cause a denial of service. IBM X-Force ID: 267970. **CVE ID : CVE-2023-45172**	https://www.ibm.com/support/pages/node/7099314, https://exchange.xforce.ibmcloud.com/vulnerabilities/267970	O-IBM-AIX-170124/977
Affected Version(s): 7.3					
N/A	22-Dec-2023	5.5	IBM AIX 7.2 and 7.3 could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of	https://www.ibm.com/support/pages/node/7100970, https://exchange.xforce.ibmcloud.com/vulnerabilities/267963	O-IBM-AIX-170124/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. IBM X-Force ID: 267963. **CVE ID : CVE-2023-45165**		
N/A	19-Dec-2023	5.5	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in AIX windows to cause a denial of service. IBM X-Force ID: 267970. **CVE ID : CVE-2023-45172**	https://www.ibm.com/support/pages/node/7099314, https://exchange.xforce.ibmcloud.com/vulnerabilities/267970	O-IBM-AIX-170124/979
Vendor: lancom-systems					
Product: lanconfig					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-LAN-LANC-170124/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: lcos					
Affected Version(s): * Up to (including) 3.66.4					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-LAN-LCOS-170124/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: lcos_fx					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP),	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-LAN-LCOS-170124/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: lcos_lx					
Affected Version(s): -					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-LAN-LCOS-170124/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Product: lcos_sx					
Affected Version(s): 4.20					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-LAN-LCOS-170124/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Affected Version(s): 5.20					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-LAN-LCOS-170124/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-48795		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2023	9.1	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view modify files on the system. IBM X-Force ID: 271196. **CVE ID : CVE-2023-47702**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271196	O-LIN-LINU-170124/986
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to upload files of a dangerous file type. IBM X-Force ID: 271341. **CVE ID : CVE-2023-47706**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271341	O-LIN-LINU-170124/987
Use of Hard-coded Credentials	20-Dec-2023	7.5	IBM Security Guardium Key Lifecycle Manager 4.3 contains plain text hard-coded credentials or	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmclou	O-LIN-LINU-170124/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other secrets in source code repository. IBM X-Force ID: 271220. **CVE ID : CVE-2023-47704**	d.com/vulnerabilities/271220	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	IBM Security Guardium Key Lifecycle Manager 4.3 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: 271522. **CVE ID : CVE-2023-47707**	https://www.ibm.com/support/pages/node/7091157	O-LIN-LINU-170124/989
Generation of Error Message Containing Sensitive Information	20-Dec-2023	5.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271197	O-LIN-LINU-170124/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			system. IBM X-Force ID: 271197. **CVE ID : CVE-2023-47703**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-Dec-2023	5.3	When resolving a symlink, a race may occur where the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121. **CVE ID : CVE-2023-6857**	https://www.mozilla.org/security/advisories/mfsa2023-54/, https://www.mozilla.org/security/advisories/mfsa2023-55/, https://www.mozilla.org/security/advisories/mfsa2023-56/	O-LIN-LINU-170124/991
Improper Input Validation	20-Dec-2023	4.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to manipulate username data due to improper input validation. IBM X-Force ID: 271228. **CVE ID : CVE-2023-47705**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271228	O-LIN-LINU-170124/992
Affected Version(s): 6.7					
Use After Free	18-Dec-2023	7.8	A use-after-free vulnerability in the	https://git.kernel.org/pub/scm	O-LIN-LINU-170124/993

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a. **CVE ID : CVE-2023-6817**	/linux/kernel/git/torvalds/linux.git/commit/?id=317eb9685095678f2c9f5a8189de698c5354316a, https://kernel.dance/317eb9685095678f2c9f5a8189de698c5354316a	
Affected Version(s): From (including) 2.6.12 Up to (excluding) 6.7					
Use After Free	19-Dec-2023	7	A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=e2b706c691905fe78468c361aaabc719d0a496f1,	O-LIN-LINU-170124/994

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread. We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1. **CVE ID : CVE-2023-6932**	https://kernel.dance/e2b706c691905fe78468c361aaabc719d0a496f1	
Affected Version(s): From (including) 4.3 Up to (excluding) 6.7					
Out-of-bounds Write	19-Dec-2023	7.8	A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation. A perf_event's read_size can overflow, leading to an heap out-of-bounds increment	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=382c27f4ed28f803b1f1473ac2d8db0afc795a1b, https://kernel.dance/382c27f4ed28f803b1f1473ac2d8db0afc795a1b	O-LIN-LINU-170124/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or write in perf_read_group(). We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b. **CVE ID : CVE-2023-6931**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.143					
Use After Free	18-Dec-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. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=317eb968509567 8f2c9f5a8189de698c5354316a, https://kernel.dance/317eb9685095678f2c9f5a8189de698c5354316a	O-LIN-LINU-170124/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			317eb9685095678f2c9f5a8189de698c5354316a. **CVE ID : CVE-2023-6817**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.68					
Use After Free	18-Dec-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. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=317eb9685095678f2c9f5a8189de698c5354316a, https://kernel.dance/317eb9685095678f2c9f5a8189de698c5354316a	O-LIN-LINU-170124/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-6817		
Affected Version(s): From (including) 5.6 Up to (excluding) 5.10.204					
Use After Free	18-Dec-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. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a. **CVE ID : CVE-2023-6817**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=317eb9685095678f2c9f5a8189de698c5354316a, https://kernel.dance/317eb9685095678f2c9f5a8189de698c5354316a	O-LIN-LINU-170124/998
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.7					
Use After Free	18-Dec-2023	7.8	A use-after-free vulnerability in the Linux kernel's	https://git.kernel.org/pub/scm/linux/kernel/g	O-LIN-LINU-170124/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netfilter: nf_tables component can be exploited to achieve local privilege escalation. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a. **CVE ID : CVE-2023-6817**	it/torvalds/linux.git/commit/?id=317eb9685095678f2c9f5a8189de698c5354316a, https://kernel.dance/317eb9685095678f2c9f5a8189de698c5354316a	
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Missing Authentication for Critical Function	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before on Windows and 2.6.9 and before on	N/A	O-MIC-WIND-170124/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS, allows attackers to bypass network filtering, execute arbitrary code, and obtain sensitive information via DarkLayer Guard threat prevention module. **CVE ID : CVE-2023-29485**		
N/A	21-Dec-2023	9.8	An issue was discovered in Heimdal Thor agent versions 3.4.2 and before 3.7.0 on Windows, allows attackers to bypass USB access restrictions, execute arbitrary code, and obtain sensitive information via Next-Gen Antivirus component. **CVE ID : CVE-2023-29486**	N/A	O-MIC-WIND-170124/1001
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-41727		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46216**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1003
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46217**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1004
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46220		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46221**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1006
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46222**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1007
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46223		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46224**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1009
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46225**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1010
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46257		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46258**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1012
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46259**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1013
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1014

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46260		
Out-of-bounds Write	19-Dec-2023	9.8	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution. **CVE ID : CVE-2023-46261**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1015
Unrestricted Upload of File with Dangerous Type	19-Dec-2023	9.8	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remote code execution. **CVE ID : CVE-2023-46263**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1016
Unrestricted Upload of File with Dangerous Type	19-Dec-2023	9.8	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remove code execution. **CVE ID : CVE-2023-46264**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2023	9.1	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view modify files on the system. IBM X-Force ID: 271196. **CVE ID : CVE-2023-47702**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271196	O-MIC-WIND-170124/1018
Unrestricted Upload of File with Dangerous Type	20-Dec-2023	8.8	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to upload files of a dangerous file type. IBM X-Force ID: 271341. **CVE ID : CVE-2023-47706**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271341	O-MIC-WIND-170124/1019
Out-of-bounds Write	19-Dec-2023	7.5	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS).	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1020

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-46803		
Out-of-bounds Write	19-Dec-2023	7.5	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS). **CVE ID : CVE-2023-46804**	https://download.wavelink.com/Files/avalanche_v6.4.2_release_notes.txt	O-MIC-WIND-170124/1021
Use of Hard-coded Credentials	20-Dec-2023	7.5	IBM Security Guardium Key Lifecycle Manager 4.3 contains plain text hard-coded credentials or other secrets in source code repository. IBM X-Force ID: 271220. **CVE ID : CVE-2023-47704**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271220	O-MIC-WIND-170124/1022
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2023	5.4	IBM Security Guardium Key Lifecycle Manager 4.3 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	https://www.ibm.com/support/pages/node/7091157	O-MIC-WIND-170124/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 271522. **CVE ID : CVE-2023-47707**		
Generation of Error Message Containing Sensitive Information	20-Dec-2023	5.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 271197. **CVE ID : CVE-2023-47703**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271197	O-MIC-WIND-170124/1024
Improper Input Validation	20-Dec-2023	4.3	IBM Security Guardium Key Lifecycle Manager 4.3 could allow an authenticated user to manipulate username data due to improper input validation. IBM X-Force ID: 271228. **CVE ID : CVE-2023-47705**	https://www.ibm.com/support/pages/node/7091157, https://exchange.xforce.ibmcloud.com/vulnerabilities/271228	O-MIC-WIND-170124/1025
Vendor: Moxa					
Product: iologik_e1210_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request	23-Dec-2023	8.8	A Cross-Site Request Forgery	https://www.moxa.com/en/su	O-MOX-IOLO-170124/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			(CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	pport/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	
Product: iologik_e1211_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	O-MOX-IOLO-170124/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**		
Product: iologik_e1212_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user.	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	O-MOX-IOLO-170124/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-5961		
Product: iologik_e1213_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	O-MOX-IOLO-170124/1029
Product: iologik_e1214_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-	O-MOX-IOLO-170124/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	235250-iologik-e1200-series-web-server-vulnerability	
Product: iologik_e1240_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request.	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	O-MOX-IOLO-170124/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**		
Product: iologik_e1241_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	O-MOX-IOLO-170124/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: iologik_e1242_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	O-MOX-IOLO-170124/1033
Product: iologik_e1260_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-	O-MOX-IOLO-170124/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**	web-server-vulnerability	
Product: iologik_e1262_firmware					
Affected Version(s): * Up to (excluding) 3.3					
Cross-Site Request Forgery (CSRF)	23-Dec-2023	8.8	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in ioLogik E1200 Series firmware versions v3.3 and prior. An attacker can exploit this vulnerability to trick a client into making an unintentional request to the web server, which will be treated as an authentic request. This vulnerability may lead an attacker to perform	https://www.moxa.com/en/support/product-support/security-advisory/mpsa-235250-iologik-e1200-series-web-server-vulnerability	O-MOX-IOLO-170124/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operations on behalf of the victimized user. **CVE ID : CVE-2023-5961**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 6.0					
Out-of-bounds Write	18-Dec-2023	5.5	An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash. **CVE ID : CVE-2023-6228**	https://access.redhat.com/security/cve/CVE-2023-6228, https://bugzilla.redhat.com/show_bug.cgi?id=2240995	O-RED-ENTE-170124/1036
Affected Version(s): 7.0					
Out-of-bounds Write	18-Dec-2023	5.5	An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash. **CVE ID : CVE-2023-6228**	https://access.redhat.com/security/cve/CVE-2023-6228, https://bugzilla.redhat.com/show_bug.cgi?id=2240995	O-RED-ENTE-170124/1037
Affected Version(s): 8.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-Dec-2023	7.8	A vulnerability was found in perl. This issue occurs when a crafted regular expression is compiled by perl, which can allow an attacker controlled byte buffer overflow in a heap allocated buffer. **CVE ID : CVE-2023-47038**	https://access.redhat.com/security/cve/CVE-2023-47038, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1056746	O-RED-ENTE-170124/1038
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	O-RED-ENTE-170124/1039
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.c	O-RED-ENTE-170124/1040

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in	om/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4,		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Out-of-bounds Write	18-Dec-2023	5.5	An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash. **CVE ID : CVE-2023-6228**	https://access.redhat.com/security/cve/CVE-2023-6228, https://bugzilla.redhat.com/show_bug.cgi?id=2240995	O-RED-ENTE-170124/1041
Affected Version(s): 9.0					
Out-of-bounds Write	18-Dec-2023	7.8	A vulnerability was found in perl. This issue occurs when a crafted regular	https://access.redhat.com/security/cve/CVE-2023-47038,	O-RED-ENTE-170124/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			expression is compiled by perl, which can allow an attacker controlled byte buffer overflow in a heap allocated buffer. **CVE ID : CVE-2023-47038**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1056746	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2023	6.3	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path. **CVE ID : CVE-2023-5115**	https://access.redhat.com/errata/RHSA-2023:5701, https://access.redhat.com/errata/RHSA-2023:5758, https://access.redhat.com/security/cve/CVE-2023-5115	O-RED-ENTE-170124/1043
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627	O-RED-ENTE-170124/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2,	bf0a6f01c1f69e8ef1d4f05d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Out-of-bounds Write	18-Dec-2023	5.5	An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash. **CVE ID : CVE-2023-6228**	https://access.redhat.com/security/cve/CVE-2023-6228, https://bugzilla.redhat.com/show_bug.cgi?id=2240995	O-RED-ENTE-170124/1045
Missing Authorization	18-Dec-2023	4.1	A flaw was found in the Skupper operator, which may permit a certain configuration to create a service account that would allow an authenticated	https://access.redhat.com/errata/RHSA-2023:6219, https://access.redhat.com/security/cve/CVE-2023-5056	O-RED-ENTE-170124/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker in the adjacent cluster to view deployments in all namespaces in the cluster. This issue permits unauthorized viewing of information outside of the user's purview. **CVE ID : CVE-2023-5056**		
Product: linux					
Affected Version(s): -					
Out-of-bounds Write	18-Dec-2023	7.5	A vulnerability was found in OpenImageIO, where a heap buffer overflow exists in the src/gif.imageio/gifinput.cpp file. This flaw allows a remote attacker to pass a specially crafted file to the application, which triggers a heap-based buffer overflow and could cause a crash, leading to a denial of service. **CVE ID : CVE-2023-3430**	N/A	O-RED-LINU-170124/1047
Vendor: ruijie					
Product: rg-ws6008_firmware					
Affected Version(s): 11.9\\(6\\)w3b2_g2c6-01_10221911					
Improper Neutralizat	20-Dec-2023	9.8	Ruijie WS6008 v1.x v2.x	N/A	O-RUI-RG-W-170124/1048

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			AC_RGOS11.9(6)W3B2_G2C6-01_10221911 and WS6108 v1.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 was discovered to contain a command injection vulnerability via the function downFiles. **CVE ID : CVE-2023-50993**		
Product: rg-ws6108_firmware					
Affected Version(s): 11.9\\(6\\)w3b2_g2c6-01_10221911					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Dec-2023	9.8	Ruijie WS6008 v1.x v2.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 and WS6108 v1.x AC_RGOS11.9(6)W3B2_G2C6-01_10221911 was discovered to contain a command injection vulnerability via the function downFiles. **CVE ID : CVE-2023-50993**	N/A	O-RUI-RG-W-170124/1049
Vendor: Tenda					
Product: i29_firmware					
Affected Version(s): 1.0.0.2					
Improper Neutralization of Special	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a command	N/A	O-TEN-I29_-170124/1050

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			injection vulnerability via the sysScheduleRebootSet function. **CVE ID : CVE-2023-50983**		
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the ip parameter in the spdtstConfigAndStart function. **CVE ID : CVE-2023-50984**	N/A	O-TEN-I29_-170124/1051
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the lanGw parameter in the lanCfgSet function. **CVE ID : CVE-2023-50985**	N/A	O-TEN-I29_-170124/1052
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the time parameter in the sysLogin function. **CVE ID : CVE-2023-50986**	N/A	O-TEN-I29_-170124/1053
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer	N/A	O-TEN-I29_-170124/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow via the time parameter in the sysTimeInfoSet function. **CVE ID : CVE-2023-50987**		
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the bandwidth parameter in the wifiRadioSetIndoor function. **CVE ID : CVE-2023-50988**	N/A	O-TEN-I29_-170124/1055
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a command injection vulnerability via the pingSet function. **CVE ID : CVE-2023-50989**	N/A	O-TEN-I29_-170124/1056
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the rebootTime parameter in the sysScheduleRebootSet function. **CVE ID : CVE-2023-50990**	N/A	O-TEN-I29_-170124/1057
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to	N/A	O-TEN-I29_-170124/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a stack overflow via the ip parameter in the setPing function. **CVE ID : CVE-2023-50992**		
Affected Version(s): 1.0.0.5					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a command injection vulnerability via the sysScheduleRebootSet function. **CVE ID : CVE-2023-50983**	N/A	O-TEN-I29_-170124/1059
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the ip parameter in the spdtstConfigAndStart function. **CVE ID : CVE-2023-50984**	N/A	O-TEN-I29_-170124/1060
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the lanGw parameter in the lanCfgSet function. **CVE ID : CVE-2023-50985**	N/A	O-TEN-I29_-170124/1061
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to	N/A	O-TEN-I29_-170124/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a buffer overflow via the time parameter in the sysLogin function. **CVE ID : CVE-2023-50986**		
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the time parameter in the sysTimeInfoSet function. **CVE ID : CVE-2023-50987**	N/A	O-TEN-I29_-170124/1063
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a buffer overflow via the bandwidth parameter in the wifiRadioSetIndoor function. **CVE ID : CVE-2023-50988**	N/A	O-TEN-I29_-170124/1064
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a command injection vulnerability via the pingSet function. **CVE ID : CVE-2023-50989**	N/A	O-TEN-I29_-170124/1065
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to	N/A	O-TEN-I29_-170124/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a buffer overflow via the rebootTime parameter in the sysScheduleRebootSet function. **CVE ID : CVE-2023-50990**		
Out-of-bounds Write	20-Dec-2023	9.8	Tenda i29 v1.0 V1.0.0.5 was discovered to contain a stack overflow via the ip parameter in the setPing function. **CVE ID : CVE-2023-50992**	N/A	O-TEN-I29_-170124/1067
Product: m3_firmware					
Affected Version(s): 1.0.0.12\\(4856\\)					
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function formGetWeiXinConfig. **CVE ID : CVE-2023-51090**	N/A	O-TEN-M3_F-170124/1068
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function R7WebsSecurityHandler. **CVE ID : CVE-2023-51091**	N/A	O-TEN-M3_F-170124/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function upgrade. **CVE ID : CVE-2023-51092**	N/A	O-TEN-M3_F-170124/1070
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function fromSetLocalVlanInfo. **CVE ID : CVE-2023-51093**	N/A	O-TEN-M3_F-170124/1071
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a Command Execution vulnerability via the function TendaTelnet. **CVE ID : CVE-2023-51094**	N/A	O-TEN-M3_F-170124/1072
Out-of-bounds Write	26-Dec-2023	9.8	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow via the function formDelWlRfPolicy. **CVE ID : CVE-2023-51095**	N/A	O-TEN-M3_F-170124/1073
Product: w9_firmware					
Affected Version(s): 1.0.0.7\\(4456\\)_cn					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a stack overflow via the function formSetAutoPing. **CVE ID : CVE-2023-51097**	N/A	O-TEN-W9_F-170124/1074
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a command injection vulnerability via the function formSetDiagnoseInfo . **CVE ID : CVE-2023-51098**	N/A	O-TEN-W9_F-170124/1075
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a command injection vulnerability via the function formexeCommand . **CVE ID : CVE-2023-51099**	N/A	O-TEN-W9_F-170124/1076
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a command injection vulnerability via the function formGetDiagnoseInfo . **CVE ID : CVE-2023-51100**	N/A	O-TEN-W9_F-170124/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a stack overflow via the function formSetUplinkInfo. **CVE ID : CVE-2023-51101**	N/A	O-TEN-W9_F-170124/1078
Out-of-bounds Write	26-Dec-2023	9.8	Tenda W9 V1.0.0.7(4456)_CN was discovered to contain a stack overflow via the function formWifiMacFilterSet. **CVE ID : CVE-2023-51102**	N/A	O-TEN-W9_F-170124/1079
Vendor: thorntech					
Product: sftp_gateway_firmware					
Affected Version(s): * Up to (excluding) 3.4.6					
Improper Validation of Integrity Check Value	18-Dec-2023	5.9	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some	https://github.com/openssh/openssh-portable/commits/master, https://github.com/erlang/otp/blob/d1b43dc0f1361d2ad67601169e90a7fc50bb0369/lib/ssh/doc/src/notes.xml#L39-L42, https://github.com/golang/crypto/commit/9d2ee975ef9fe627bf0a6f01c1f69e8ef1d4f05d	O-THO-SFTP-170124/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust. **CVE ID : CVE-2023-48795**		
Vendor: totolink					
Product: a3700r_firmware					
Affected Version(s): 9.1.2u.5822_b20200513					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Dec-2023	9.8	There is an arbitrary command execution vulnerability in the setDiagnosisCfg function of the cstecgi .cgi of the TOTOlink A3700R router device in its firmware version V9.1.2u.5822_B20200513. **CVE ID : CVE-2023-50147**	N/A	O-TOT-A370-170124/1081
Product: a7100ru_firmware					
Affected Version(s): 7.4cu.2313_b20191024					
Buffer Copy without Checking	18-Dec-2023	9.8	A vulnerability, which was classified as critical, was found	N/A	O-TOT-A710-170124/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			in Totolink A7100RU 7.4cu.2313_B20191024. Affected is the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument flag with the input ie8 leads to buffer overflow. 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-248268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-6906**		
Product: ex1200l_firmware					
Affected Version(s): 9.3.5u.6146_b20201023					
Improper Neutralization of Special Elements used in an OS Command ('OS	22-Dec-2023	9.8	TOTOlink EX1200L V9.3.5u.6146_B20201023 is vulnerable to arbitrary command execution via the cstecgi.cgi	N/A	O-TOT-EX12-170124/1083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			setOpModeCfg interface. **CVE ID : CVE-2023-51033**		
Product: ex1800t_firmware					
Affected Version(s): 9.1.0cu.2112_b20220316					
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the lanPriDns parameter' of the setLanConfig interface of the cstecgi .cgi **CVE ID : CVE-2023-51011**	N/A	O-TOT-EX18-170124/1084
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the lanGateway parameter' of the setLanConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51012**	N/A	O-TOT-EX18-170124/1085
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the	N/A	O-TOT-EX18-170124/1086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lanNetmask parameter' of the setLanConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51013**		
N/A	22-Dec-2023	9.8	TOTOLINK EX1800T V9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the lanSecDns parameter' of the setLanConfig interface of the cstecgi .cgi **CVE ID : CVE-2023-51014**	N/A	O-TOT-EX18-170124/1087
N/A	22-Dec-2023	9.8	TOTOLINX EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to arbitrary command execution in the 'enable parameter' of the setDmzCfg interface of the cstecgi .cgi **CVE ID : CVE-2023-51015**	N/A	O-TOT-EX18-170124/1088
Improper Neutralization of Special Elements used in a Command	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the	N/A	O-TOT-EX18-170124/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Command Injection')			setRebootScheCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51016**		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the lanIp parameter' of the setLanConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51017**	N/A	O-TOT-EX18-170124/1090
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'opmode' parameter of the setWiFiApConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51018**	N/A	O-TOT-EX18-170124/1091
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'key5g' parameter of the setWiFiExtenderCo	N/A	O-TOT-EX18-170124/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51019**		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the ‘langType’ parameter of the setLanguageCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51020**	N/A	O-TOT-EX18-170124/1093
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the ‘merge’ parameter of the setRptWizardCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51021**	N/A	O-TOT-EX18-170124/1094
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the ‘langFlag’ parameter of the setLanguageCfg	N/A	O-TOT-EX18-170124/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface of the cstecgi .cgi. **CVE ID : CVE-2023-51022**		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to arbitrary command execution in the 'host_time' parameter of the NTPSyncWithHost interface of the cstecgi .cgi. **CVE ID : CVE-2023-51023**	N/A	O-TOT-EX18-170124/1096
N/A	22-Dec-2023	9.8	TOTOlink EX1800T v9.1.0cu.2112_B20 220316 is vulnerable to unauthorized arbitrary command execution in the 'tz' parameter of the setNtpCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51024**	N/A	O-TOT-EX18-170124/1097
N/A	22-Dec-2023	9.8	TOTOlink EX1800T V9.1.0cu.2112_B20 220316 is vulnerable to an unauthorized arbitrary command execution in the 'admuser' parameter of the setPasswordCfg interface of the cstecgi .cgi.	N/A	O-TOT-EX18-170124/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-51025		
N/A	22-Dec-2023	9.8	TOTOlink EX1800T V9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'hour' parameter of the setRebootScheCfg interface of the cstecgi .cgi. **CVE ID : CVE-2023-51026**	N/A	O-TOT-EX18-170124/1099
N/A	22-Dec-2023	9.8	TOTOlink EX1800T V9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the 'apcliAuthMode' parameter of the setWiFiExtenderConfig interface of the cstecgi .cgi. **CVE ID : CVE-2023-51027**	N/A	O-TOT-EX18-170124/1100
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Dec-2023	9.8	TOTOLINK EX1800T 9.1.0cu.2112_B20220316 is vulnerable to unauthorized arbitrary command execution in the apcliChannel parameter of the setWiFiExtenderCo	N/A	O-TOT-EX18-170124/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfig interface of the cstecgi.cgi. **CVE ID : CVE-2023-51028**		
Vendor: weintek					
Product: cmt2078x_firmware					
Affected Version(s): 2.1.3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2023	8.8	An authenticated command injection vulnerability in Weintek cMT2078X easyweb Web Version v2.1.3, OS v20220215 allows attackers to execute arbitrary code or access sensitive information via injecting a crafted payload into the HMI Name parameter. **CVE ID : CVE-2023-50466**	N/A	O-WEI-CMT2-170124/1102