



Your Security Rabbits report for February 04, 2022

Hot topics

Nothing today

News



Threatpost

'Long Live Log4Shell': CVE-2021-44228 Not Dead Yet

The ubiquitous Log4j bug will be with us for years. John Hammond, senior security researcher at Huntress, discusses what's next.



Cyware
News -
Latest Cyber
News

Airport Services Firm Faces Cyberattack Resulting in Flight Delays Due to Impact on IT Infrastructure

Swiss airport management service Swissport reported a ransomware attack affecting its IT systems on Friday. The company said its IT infrastructure was targeted by the ransomware attack.



Threatpost

Argo CD Security Bug Opens Kubernetes Cloud Apps to Attackers

The popular continuous-delivery platform has a path-traversal bug (CVE-2022-24348) that could allow cyberattackers to hop from one application ecosystem to another.



Cyware
News -
Latest Cyber
News

AsyncRAT Operators Adopt New Evasive Delivery Technique

Morphisec identified a new sophisticated campaign using a phishing tactic with an HTML attachment to deliver AsyncRAT for around five months. Moreover, the malware campaign has one of the lowest detection rates, according to VirusTotal. This calls upon the organizations to regularly audit and upgrade their security posture to stay protected.



Cyware
News -
Latest Cyber
News

China-linked Cyberattack on News Corp Resulted in the Compromise of Employee Emails

The attack, which was discovered on January 20, affected Dow Jones, the Wall Street Journal, the New York Post, News Corp headquarters, and its UK news operations, according to the report.



Cyware
News -
Latest Cyber
News

CISA orders federal agencies to patch actively exploited Windows bug

The Cybersecurity and Infrastructure Security Agency (CISA) has ordered federal agencies to patch their systems against an actively exploited Windows vulnerability that enables attackers to gain SYSTEM privileges.



Cyware
News -
Latest Cyber

Distrust, feuds building among ransomware groups

In an industry that operates in anonymity, trust is everything -- but recent accusations of ransomware actors working with or being law enforcement is threatening that work model.



Security
Affairs

A nation-state actor hacked media and publishing giant News Corp

American media and publishing giant News Corp revealed it was victim of a cyber attack from an advanced persistent threat actor. American media and publishing giant News Corp revealed it was victim of a cyber attack from an advanced persistent threat actor that took place in January. The attackers compromised one of the systems of the [...] The post A nation-state actor hacked media and publishing giant News Corp appeared first on Security Affairs.



The Hacker
News

Another Israeli Firm, QuaDream, Caught Weaponizing iPhone Bug for Spyware

A now-patched security vulnerability in Apple iOS that was previously found to be exploited by Israeli company NSO Group was also separately weaponized by a different surveillance vendor named QuaDream to hack into the company's devices. The development was reported by Reuters, citing unnamed sources, noting that "the two rival businesses gained the same ability last year to remotely break into



Cyware
News -
Latest Cyber
News

Argo CD vulnerability leaks sensitive info from Kubernetes apps

A vulnerability in Argo CD, used by thousands of orgs for deploying applications to Kubernetes, can be leveraged in attacks to disclose sensitive information such as passwords and API keys.



Threatpost

Attackers Target Intuit Users by Threatening to Cancel Tax Accounts

The usual tax-season barrage of cybercriminal activity is already underway with a phishing campaign impersonating the popular accounting and tax-filing software.



ZDNet |
security RSS

CISA issues advisory warning of critical vulnerabilities in Airspan Networks Mimosa

The vulnerabilities go all the way up to 10 on the CVSS severity score.



The Hacker
News

CISA Warns of Critical Vulnerabilities Discovered in Airspan Networks Mimosa

















The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday published an Industrial Controls Systems Advisory (ICSA) warning of multiple vulnerabilities in the Airspan Networks Mimosa equipment that could be abused to gain remote code execution, create a denial-of-service (DoS) condition, and obtain sensitive information. "Successful exploitation of these vulnerabilities could



IT Security
Guru

Edgescan partners with Manicode to revolutionise secure coding courses

Edgescan, the provider of the most comprehensive fullstack vulnerability management solution, today announces a partnership with Manicode Security, the secure coding education company. With a combination of lecture, security testing demonstration, and code review, Manicode classes are sure to entertain and educate app, web services, and mobile software developers and architects to the practices of [...] The

<div>News</div>		<p>post Edgescan partners with Manicode to revolutionise secure coding courses appeared first on IT Security Guru.</p>
<div> <div>  <div> <div>CYWARE</div> <div>SOCIAL</div> </div> </div> <div> <div>Cyware</div> <div>News - Latest Cyber News</div> </div> </div>	<p>Google Drive integration errors created SSRF flaws in multiple applications Implementation flaws in Google Drive integrations created server-side request forgery (SSRF) vulnerabilities in a variety of applications, a security researcher has revealed.</p>	<div> <div>  <div> <div>The Hacker News</div> </div> </div> <div> <div>The Hacker News</div> </div> </div> <p>Hackers Exploited 0-Day Vulnerability in Zimbra Email Platform to Spy on Users A threat actor, likely Chinese in origin, is actively attempting to exploit a zero-day vulnerability in the Zimbra open-source email platform as part of spear-phishing campaigns that commenced in December 2021. The espionage operation -- codenamed "EmailThief" -- was detailed by cybersecurity company Volexity in a technical report published Thursday, noting that successful exploitation of the</p>
<div> <div>  <div> <div>CYWARE</div> <div>SOCIAL</div> </div> </div> <div> <div>Cyware</div> <div>News - Latest Cyber News</div> </div> </div>	<p>How attackers got access to the systems of the National Games of China In early September 2021, Avast threat researcher David Alvarez found a malware sample with a suspicious file extension and a report submitted by the National Games IT team to VirusTotal on an attack against a server associated with the Games.</p>	<div> <div>  <div> <div>Security Affairs</div> </div> </div> <div> <div>Security Affairs</div> </div> </div> <p>Microsoft blocked tens of billions of brute-force and phishing attacks in 2021 Office 365 and Azure Active Directory (Azure AD) customers were the targets of billions of brute-force and phishing attacks last year. Microsoft revealed that Office 365 and Azure Active Directory (Azure AD) customers were the targets of billions of phishing emails and brute force attacks last year. The IT giant added has blocked more than 25.6 billion Azure AD [...] The post Microsoft blocked tens of billions of brute-force and phishing attacks in 2021 appeared first on Security Affairs.</p>
<div> <div>  <div> <div>CYWARE</div> <div>SOCIAL</div> </div> </div> <div> <div>Cyware</div> <div>News - Latest Cyber News</div> </div> </div>	<p>Microsoft: Russian FSB hackers hitting Ukraine since October Microsoft said today that a Russian hacking group known as Gamaredon has been behind a streak of spear-phishing emails targeting Ukrainian entities and organizations related to Ukrainian affairs since October 2021.</p>	<div> <div>  <div> <div>CYWARE</div> <div>SOCIAL</div> </div> </div> <div> <div>Cyware</div> <div>News - Latest Cyber News</div> </div> </div> <p>Millions of Android Users Targeted by Dark Herring Experts exposed Dark Herring subscription fraud campaign that infected 105 million devices worldwide via 500 malicious apps to steal hundreds of millions of dollars from unsuspecting users. The names of some malicious apps are Smashex, Upgradem, Stream HD, Vidly Vibe, and Cast It. This indicates that sometimes downloading apps from genuine stores does not guarantee the safety of users.</p>
<div> <div>  <div> <div>CYWARE</div> <div>SOCIAL</div> </div> </div> <div> <div>Cyware</div> <div>News - Latest Cyber News</div> </div> </div>	<p>Multiple India-based call centers and their directors indicted for perpetuating phone scams affecting thousands of Americans The US Justice Department indicted six India-based call centers and their directors for their alleged role in making tens of millions of scam calls to defraud thousands of American citizens.</p>	<div> <div>  <div> <div>FLASHPOINT</div> </div> </div> <div> <div>Blog à€” Flashpoint</div> </div> </div> <p>New Report From Flashpoint and Risk Based Security Finds 22 Billion Records Exposed in 2021 Data Breaches Today, Risk Based Security's annual Data Breach QuickView Report was released, from Inga Goddjin, Executive Vice President of RBS, and featuring quantitative research from Ashley Allocca, Cybersecurity Intelligence Analyst at Flashpoint. Powered by Cyber Risk Analytics, our annual report outlines some of the year's most notable trends in breach activity across a variety of industries. [...] The post New Report From Flashpoint and Risk Based Security Finds 22 Billion Records Exposed in 2021 Data Breaches appeared first on Flashpoint.</p>
<div> <div>  <div> <div>ZDNet</div> </div> </div> <div> <div>ZDNet security RSS</div> </div> </div>	<p>Operation EmailThief: Zero-day XSS vulnerability in Zimbra email platform revealed A zero-day bug in the Zimbra email platform is reportedly under attack.</p>	<div> <div>  <div> <div>Security Affairs</div> </div> </div> <div> <div>Security Affairs</div> </div> </div> <p>Over 500,000 people were impacted by a ransomware attack that hit Morley Business services firm Morley was hit by a ransomware attack that may have exposed data of +500,000 individuals. Business services company Morley was victim of a ransomware attack that may have resulted in a data breach impacting more than 500,000 individuals. Morley Companies is a United States corporation that provides business services to Fortune 500 and Global 100 clients; contact [...] The post Over 500,000 people were impacted by a ransomware attack that hit Morley appeared first on Security Affairs.</p>
<div> <div>  <div> <div>IT SECURITY</div> <div>GURU</div> </div> </div> <div> <div>IT Security Guru</div> </div> </div>	<p>Pharma employee credentials exposed Employees and executives from the top 20 pharma companies on the Fortune 500 list have had their credentials exposed, new research suggests. Constella Intelligence identified 9,030 breaches/leakages and 4,549,871 exposed records—including attributes like email addresses, passwords, phone numbers, addresses, and even credit card and banking information--related to employee corporate credentials from the companies analysed. The circulation [...] The post Pharma employee credentials exposed appeared first on IT Security Guru.</p>	<div> <div>  <div> <div>Security Affairs</div> </div> </div> <div> <div>Security Affairs</div> </div> </div> <p>Ransomware attack hit Swissport International causing delays in flights Aviation services company Swissport International was hit by a ransomware attack that impacted its operations. Swissport International Ltd. is an aviation services company providing airport ground,lounge hospitality and cargo handling services owned by an international group of investors. The company handles around 282 million passengers and 4.8 million tonnes of cargo annually, on behalf of [...] The post Ransomware attack hit Swissport International causing delays in flights appeared first on Security Affairs.</p>
<div> <div>  <div> <div>CYWARE</div> <div>SOCIAL</div> </div> </div> <div> <div>Cyware</div> <div>News - Latest Cyber News</div> </div> </div>	<p>Ransomware attack hit Swissport International causing delays in flights Swissport International was hit by a ransomware attack that had a severe impact on its operations causing flights to suffer delays. The company said via Twitter that the attack has been largely contained.</p>	<div> <div>  <div> <div>IT SECURITY</div> <div>GURU</div> </div> </div> <div> <div>IT Security Guru</div> </div> </div> <p>Ransomware gangs and supply chain vulnerabilities: Nozomi Networks Labs reports on the current threat landscape While vulnerability disclosures increased 21% in the second half of 2021 and increasingly sophisticated criminal attacks made regular news, organizations are fighting back with targeted remediation efforts A new OT/IoT security trends report from Nozomi Networks Labs finds cyber threats have becoming a never-ending reality for critical business operations. In a review of the threat [...] The post Ransomware gangs and supply chain vulnerabilities: Nozomi Networks Labs reports on the current threat landscape appeared first on IT Security Guru.</p>
<div> <div>  <div> <div>cyberscoop</div> </div> </div> <div> <div>CyberScoop</div> </div> </div>	<p>Ransomware spree hitting European oil, transport companies European oil and transportation services have spent all week under attack by ransomware. The latest victim, aviation services company Swissport, announced Friday that ransomware struck part of its IT infrastructure, causing flight delays and knocking</p>	<div> <div>  <div> <div>Security Affairs</div> </div> </div> <div> <div>Security Affairs</div> </div> </div> <p>Retail giant Target open sources Merry Maker e-skimmer detection tool Retail giant Target is going to open-source an internal tool, dubbed Merry Maker, designed to detect e-skimming attacks.</p>

its website offline. The company said last month that in 2019, it fueled 2.3 million flights, and claims 2,000 employees at 40 airports across six countries. A part of #Swissport's IT infrastructure was subject to a ransomware attack. The attack has been largely contained, and we are working actively to fully resolve the issue as quickly as possible. Swissport regrets any impact the incidence has had on our service delivery. -- Swissport (@swis[...]

Affairs

Retail giant Target announced the release in open-source of an internal tool, dubbed Merry Maker, designed to detect e-skimming attacks. Merry Maker is a tool designed by Target security developers Eric Brandel and Caleb Walch (@ebrandel and @cawalch) to [...] The post Retail giant Target open sources Merry Maker e-skimmer detection tool appeared first on Security Affairs.



Security
Affairs

Russia-linked Gamaredon APT targeted a western government entity in Ukraine

The Russia-linked Gamaredon APT group attempted to compromise an unnamed Western government entity in Ukraine. Palo Alto Networks' Unit 42 reported that the Russia-linked Gamaredon APT group attempted to compromise an unnamed Western government entity operating in Ukraine in January, while geopolitical tensions between Russia and Ukraine have escalated dramatically. In Mid January the Ukrainian [...] The post Russia-linked Gamaredon APT targeted a western government entity in Ukraine appeared first on Security Affairs.



CyberScoop

Russia-linked Gamaredon shows signs of possible recent activity in Ukraine, researchers say

A series of cyberattacks on Ukrainian institutions over the past few weeks -- including website defacement, computer-wiping malware and phishing campaigns -- have the hallmarks of hacking activity associated with the Russian government, but conclusive attribution remains elusive. Research published Thursday, however, shows how a known Russia-linked hacking group, Gamaredon, could be involved in active targeting of Ukrainian targets, including an attempt to compromise a Western government entity in Ukraine on Jan. 19. The findings, published by Palo Alto Networks' Unit 42 threat intelligence unit, focus on the group as the Russian military amasses more than 100,000 troops along its border wit[...]



IT Security
Guru

Russia-Ukraine escalation of tensions: FBI calls for reports of uptick in cyber activit

The FBI is asking US businesses to report any uptick in Russian hacking threats -- the latest effort to prepare for potential Russian cyberattacks on US organizations amid Russia's troop buildup on Ukraine's border, CNN reported this week. "Have you identified any efforts by known or suspected Russian [hacking groups] to test exploitation capabilities, develop new malware [...] The post Russia-Ukraine escalation of tensions: FBI calls for reports of uptick in cyber activit appeared first on IT Security Guru.



ZDNet |
security RSS

Russian APT Primitive Bear attacks Western government department in Ukraine through job hunt

The hacking group's latest activities come at a time when tension is boiling between Russia and Ukraine.



The Hacker
News

Russian Gamaredon Hackers Targeted 'Western Government Entity' in Ukraine

The Russia-linked Gamaredon hacking group attempted to compromise an unnamed Western government entity operating in Ukraine last month amidst ongoing geopolitical tensions between the two countries. Palo Alto Networks' Unit 42 threat intelligence team, in a new report publicized on February 3, said that the phishing attack took place on January 19, adding it "mapped out three large clusters of



WeLiveSecurity

Think before you scan: How fraudsters can exploit QR codes to steal money

QR codes are all the rage and scammers have taken notice. Look out for dangers lurking behind those little black-and-white squares. The post Think before you scan: How fraudsters can exploit QR codes to steal money appeared first on WeLiveSecurity



The Hacker
News

U.S. Authorities Charge 6 Indian Call Centers Scamming Thousands of Americans

A number of India-based call centers and their directors have been indicted for their alleged role in placing tens of millions of scam calls aimed at defrauding thousands of American consumers. The indictment charged Manu Chawla, Sushil Sachdeva, Nitin Kumar Wadwani, Swarndeep Singh, Dinesh Manohar Sachdev, Gaje Singh Rathore, Sanket Modi, Rajiv Solanki and their respective call centers for



IT Security
Guru

US Federal government creates cybersecurity incident review board

The Department of Homeland Security has announced a new Cyber Safety Review Board bringing together cybersecurity experts from public and private organizations to "review and assess significant cybersecurity events." The board was part of the executive order that President Joe Biden signed last year. Experts have long called for a federal organisation for cybersecurity incidents [...] The post US Federal government creates cybersecurity incident review board appeared first on IT Security Guru.



Naked
Security

Wormhole cryptotrading company turns over \$340,000,000 to criminals

It was the best of blockchains, it was the worst of blockchains... as Charles Dickens might have said.



IT Security
Guru

Zimbra zero-day vulnerability exploited to steal emails

Attacks linked to a Chinese threat actor have exploited a Zimbra's zero-day vulnerability and are stealing emails linked to European government and media. Researchers say that at the time of writing the exploit has no available patch. Zimbra says that more than 200,000 businesses from over 140 countries are using its software, including over 1,000 [...] The post Zimbra zero-day vulnerability exploited to steal emails appeared first on IT Security Guru.















Security
Affairs

Zimbra zero-day vulnerability actively exploited by an alleged Chinese threat actor

An alleged Chinese threat actor is actively attempting to exploit a zero-day vulnerability in the Zimbra open-source email platform. An alleged Chinese threat actor, tracked as TEMP_Heretic, is actively attempting to exploit a zero-day XSS vulnerability in the Zimbra open-source email platform. The zero-day vulnerability impacts almost any Zimbra install running version 8.8.15. Researchers from [...] The post Zimbra zero-day vulnerability actively exploited by an alleged Chinese threat actor appeared first on Security Affairs.

Twitter

Potentially Critical CVE Detected! CVE-2022-24300 Description: Minetest before 5.4.0 allows attackers to add or modify arbitrary

 wuhan005	Got my first CVECVE-2022-24123	 Robo Shadow Alerts	meta fields of... CVSS: 8.82 #redhat #enterprise_linux_for #CVE #CyberSecurity #DataBreach
 Robo Shadow Alerts	Potentially Critical CVE Detected! CVE-2021-43509 Description: SQL Injection vulnerability exists in Sourcecodester Simple Client Management Sy... CVSS: 9.44 #sourcecodester #travel_management_sy #CVE #CyberSecurity #DataBreach	 Robo Shadow Alerts	Potentially Critical CVE Detected! CVE-2021-43510 Description: SQL Injection vulnerability exists in Sourcecodester Simple Client Management Sy... CVSS: 9.47 #sourcecodester #complaint_management #CVE #CyberSecurity #DataBreach
 ThreatMeter	CVE-2022-24123 MarkText through 0.16.3 does not sanitize the input of a mermaid block before rendering. This could lead to Remote Code Execution via a .md file containing a mutation Cross-Site Scripting (XSS) payload. (CVSS:0.0) (Last Update:2022-01-29)	 Robo Shadow Alerts	Potentially Critical CVE Detected! CVE-2022-0339 Description: Server-Side Request Forgery (SSRF) in Pypi calibreweb prior to 0.6.16.... CVSS: 8.56 #webp_converter_for_m #webp_converter_for_m #CVE #CyberSecurity #DataBreach
 CVE	CVE-2021-46660 Signiant Manager+Agents before 15.1 allows XML External Entity (XXE) attacks.	 ThreatMeter	CVE-2022-24300 Minetest before 5.4.0 allows attackers to add or modify arbitrary meta fields of the same item stack as saved user input, aka ItemStack meta injection. (CVSS:0.0) (Last Update:2022-02-02)
 CVE	CVE-2022-0339 Server-Side Request Forgery (SSRF) in Pypi calibreweb prior to 0.6.16.	 Angenoire	#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2021-23520
 Cyber Security Bot	NA - CVE-2022-22994 - A remote code execution vulnerability was...	 CVE	CVE-2022-0401 Path Traversal in NPM w-zip prior to 1.0.12.

Source: *NIST*

NIST CVE: Critical

CVE-2022-22992	<p>A command injection remote code execution vulnerability was discovered on Western Digital My Cloud Devices that could allow an attacker to execute arbitrary system commands on the device. The vulnerability was addressed by escaping individual arguments to shell functions coming from user input.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div> </div>	CVE-2022-22994	<p>A remote code execution vulnerability was discovered on Western Digital My Cloud devices where an attacker could trick a NAS device into loading through an unsecured HTTP call. This was a result insufficient verification of calls to the device. The vulnerability was addressed by disabling checks for internet connectivity using HTTP.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div> </div>
CVE-2022-21217	<p>An out-of-bounds write vulnerability exists in the device TestEmail functionality of reolink RLC-410W v3.0.0.136 20121102. A specially-crafted network request can lead to an out-of-bounds write. An attacker can send an HTTP request to trigger this vulnerability.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div> </div>	CVE-2022-24263	<p>Hospital Management System v4.0 was discovered to contain a SQL injection vulnerability in /Hospital-Management-System-master/func.php via the email parameter.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-31</div> <div>Updated: 2022-02-04</div> </div> </div>
CVE-2022-24123	<p>MarkText through 0.16.3 does not sanitize the input of a mermaid block before rendering. This could lead to Remote Code Execution via a .md file containing a mutation Cross-Site Scripting (XSS) payload.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-29</div> <div>Updated: 2022-02-04</div> </div> </div>	CVE-2022-24300	<p>Minetest before 5.4.0 allows attackers to add or modify arbitrary meta fields of the same item stack as saved user input, aka ItemStack meta injection.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-02-02</div> <div>Updated: 2022-02-04</div> </div> </div>
CVE-2020-36064	<p>Online Course Registration v1.0 was discovered to contain hardcoded credentials in the source code which allows attackers access to the control panel if compromised.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-31</div> <div>Updated: 2022-02-04</div> </div> </div>	CVE-2022-0401	<p>Path Traversal in NPM w-zip prior to 1.0.12.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div> </div>
CVE-2022-0339	<p>Server-Side Request Forgery (SSRF) in Pypi calibreweb prior to 0.6.16.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-30</div> <div>Updated: 2022-02-04</div> </div> </div>	CVE-2021-46660	<p>Signiant Manager+Agents before 15.1 allows XML External Entity (XXE) attacks.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-01-30</div> <div>Updated: 2022-02-04</div> </div> </div>
CVE-2021-43509	<p>SQL Injection vulnerability exists in Sourcecodester Simple Client Management System 1.0 via the id parameter in view-service.php.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div> </div>	CVE-2021-43510	<p>SQL Injection vulnerability exists in Sourcecodester Simple Client Management System 1.0 via the username field in login.php.</p> <div> <div>CRITICAL</div> <div> <div>Vector:</div> <div>network</div> </div> <div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div> </div>

CVE-2022-0320	<p>The Essential Addons for Elementor WordPress plugin before 5.0.5 does not validate and sanitise some template data before it them in include statements, which could allow unauthenticated attackers to perform Local File Inclusion attack and read arbitrary files on the server, this could also lead to RCE via user uploaded files or other LFI to RCE techniques.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-23520	<p>The package juice-framework/juce before 6.1.5 are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) via the ZipFile::uncompressEntry function in juce_ZipFile.cpp. This vulnerability is triggered when the archive is extracted upon calling uncompressTo() on a ZipFile object.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-01-31</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-23484	<p>The package zip-local before 0.3.5 are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) which can lead to an extraction of a crafted file outside the intended extraction directory.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-45742	<p>TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-45733	<p>TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a command injection vulnerability in the function NTPSyncWithHost. This vulnerability allows attackers to execute arbitrary commands via the parameter host_time.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-46458	<p>Victor CMS v1.0 was discovered to contain a SQL injection vulnerability in the component admin/posts.php?source=add_post. This vulnerability can be exploited through a crafted POST request via the post_title parameter.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-01-31</div> <div>Updated: 2022-02-04</div> </div>

CVE-2021-23558	<p>The package bmoor before 0.10.1 are vulnerable to Prototype Pollution due to missing sanitization in set function. **Note:** This vulnerability derives from an incomplete fix in [CVE-2020-7736] (https://security.snyk.io/vuln/SNYK-JS-BMOOR-598664)</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-23760	<p>The package keyget from 0.0.0 are vulnerable to Prototype Pollution via the methods set, push, and at which could allow an attacker to cause a denial of service and may lead to remote code execution. **Note:** This vulnerability derives from an incomplete fix to [CVE-2020-28272](https://security.snyk.io/vuln/SNYK-JS-KEYGET-1048048)</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-24762	<p>The Perfect Survey WordPress plugin before 1.5.2 does not validate and escape the question_id GET parameter before using it in a SQL statement in the get_question AJAX action, allowing unauthenticated users to perform SQL injection.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-45740	<p>TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a stack overflow in the setWiFiWpsStart function. This vulnerability allows attackers to cause a Denial of Service (DoS) via the pin parameter.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-45738	<p>TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a command injection vulnerability in the function UploadFirmwareFile. This vulnerability allows attackers to execute arbitrary commands via the parameter FileName.</p> <div> <div>CRITICAL</div> <div>Vector: network</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div> </div>

Source: *NIST*

NIST CVE: High

CVE-2022-21801	<p>A denial of service vulnerability exists in the netserver rcv_command functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted network request can lead to a reboot. An attacker can send a malicious packet to trigger this vulnerability.</p> <div> <div>HIGH</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>
CVE-2022-21134	<p>A firmware update vulnerability exists in the "update" firmware checks functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to firmware update. An attacker can send a sequence of requests to trigger this vulnerability.</p> <div> <div>HIGH</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>
CVE-2022-22993	<p>A limited SSRF vulnerability was discovered on Western Digital My Cloud devices that could allow an attacker to impersonate a server and reach any page on the server by bypassing access controls. The vulnerability was addressed by creating a whitelist for valid parameters.</p> <div> <div></div> <div>Vector:</div> <div>Created: 2022-</div> <div>Updated: 2022-</div> </div>

CVE-2021-40419	<p>A firmware update vulnerability exists in the 'factory' binary of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted series of network requests can lead to arbitrary firmware update. An attacker can send a sequence of requests to trigger this vulnerability.</p> <div> <div>HIGH</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-41018	<p>A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests.</p> <div> <div>HIGH</div> <div>Vector: network</div> <div>Created: 2022-02-02</div> <div>Updated: 2022-02-04</div> </div>
CVE-2022-21796	<p>A memory corruption vulnerability exists in the netserver parse_command_list functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to an out-of-bounds write. An attacker can send an HTTP request to trigger this vulnerability.</p> <div> <div>HIGH</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>

	<div><div>HIGH</div><div>network</div><div>01-28</div><div>02-04</div></div>	
CVE-2021-27971	<div><p>Alps Alpine Touchpad Driver 10.3201.101.215 is vulnerable to DLL Injection.</p><div><div>HIGH</div><div>Vector: local</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div></div>	<div><div>CVE-2021-34805</div><div><p>An issue was discovered in FAUST iServer before 9.0.019.019.7. For each URL request, it accesses the corresponding .fau file on the operating system without preventing %2e%2e%5c directory traversal.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div></div></div>
CVE-2021-44255	<div><p>Authenticated remote code execution in MotionEye <= 0.42.1 and MotioneEyeOS <= 20200606 allows a remote attacker to upload a configuration backup file containing a malicious python pickle file which will execute arbitrary code on the server.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div></div>	<div><div>CVE-2022-22510</div><div><p>Codesys Profinet in version V4.2.0.0 is prone to null pointer dereference that allows a denial of service (DoS) attack of an unauthenticated user via SNMP.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-02</div><div>Updated: 2022-02-04</div></div></div></div>
CVE-2022-23597	<div><p>Element Desktop is a Matrix client for desktop platforms with Element Web at its core. Element Desktop before 1.9.7 is vulnerable to a remote program execution bug with user interaction. The exploit is non-trivial and requires clicking on a malicious link, followed by another button click. To the best of our knowledge, the vulnerability has never been exploited in the wild. If you are using Element Desktop < 1.9.7, we recommend upgrading at your earliest convenience. If successfully exploited, the vulnerability allows an attacker to specify a file path of a binary on the victim's computer which then gets executed. Notably, the attacker does *not* have the ability to specify program arguments. However, in certain unspecified configurations, the attacker may be able to specify an URI instead of a file path which then gets handled using standard platform mechanisms. These may allow exploiting further vulnerabilities in those mechanisms, potentially leading to arbitrary code execution.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div></div>	<div><div>CVE-2022-0407</div><div><p>Heap-based Buffer Overflow in Conda vim prior to 8.2.</p><div><div>HIGH</div><div>Vector: local</div><div>Created: 2022-01-30</div><div>Updated: 2022-02-04</div></div></div></div>
CVE-2021-41040	<div><p>In Eclipse Wakaama, ever since its inception until 2021-01-14, the CoAP parsing code does not properly sanitize network-received data.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div></div>	<div><div>CVE-2021-46101</div><div><p>In Git for windows through 2.34.1 when using git pull to update the local warehouse, git.cmd can be run directly.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div></div></div>
CVE-2022-23596	<div><p>Junrar is an open source java RAR archive library. In affected versions A carefully crafted RAR archive can trigger an infinite loop while extracting said archive. The impact depends solely on how the application uses the library, and whether files can be provided by malignant users. The problem is patched in 7.4.1. There are no known workarounds and users are advised to upgrade as soon as possible.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div></div>	<div><div>CVE-2022-24122</div><div><p>kernel/ucount.c in the Linux kernel 5.14 through 5.16.4, when unprivileged user namespaces are enabled, allows a use-after-free and privilege escalation because a ucounts object can outlive its namespace.</p><div><div>HIGH</div><div>Vector: local</div><div>Created: 2022-01-29</div><div>Updated: 2022-02-04</div></div></div></div>
CVE-2022-21721	<div><p>Next.js is a React framework. Starting with version 12.0.0 and prior to version 12.0.9, vulnerable code could allow a bad actor to trigger a denial of service attack for anyone using i18n functionality. In order to be affected by this CVE, one must use next start or a custom server and the built-in i18n support. Deployments on Vercel, along with similar environments where invalid requests are filtered before reaching Next.js, are not affected. A patch has been released, `next@12.0.9`, that mitigates this issue. As a workaround, one may ensure `/\${locale}/_next/` is blocked from reaching the Next.js instance until it becomes feasible to upgrade.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div></div>	<div><div>CVE-2022-23602</div><div><p>Nimforum is a lightweight alternative to Discourse written in Nim. In versions prior to 2.2.0 any forum user can create a new thread/post with an include referencing a file local to the host operating system. Nimforum will render the file if able. This can also be done silently by using NimForum's post "preview" endpoint. Even if NimForum is running as a non-critical user, the forum.json secrets can be stolen. Version 2.2.0 of NimForum includes patches for this vulnerability. Users are advised to upgrade as soon as is possible. There are no known workarounds for this issue.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div></div></div>
CVE-2022-0408	<div><p>Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.</p><div><div>HIGH</div><div>Vector: local</div><div>Created: 2022-01-30</div><div>Updated: 2022-02-04</div></div></div>	<div><div>CVE-2021-28962</div><div><p>Stormshield Network Security (SNS) before 4.2.2 allows a read-only administrator to gain privileges via CLI commands.</p><div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div></div></div>
CVE-2021-25093	<div><p>The Link Library WordPress plugin before 7.2.8 does not have authorisation in place when deleting links, allowing unauthenticated users to delete arbitrary links</p></div>	<div><div>CVE-2021-24763</div><div><p>The Perfect Survey WordPress plugin before 1.5.2 does not have proper authorisation nor CSRF checks in the save_global_setting AJAX action, allowing unauthenticated users to edit surveys and modify settings. Given the lack of sanitisation and escaping in</p></div></div>

	<div>via a crafted request</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>
CVE-2022-24124	<div>The query API in Casdoor before 1.13.1 has a SQL injection vulnerability related to the field and value parameters, as demonstrated by api/get-organizations.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-01-29</div><div>Updated: 2022-02-04</div></div>
CVE-2021-45739	<div>TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a stack overflow in the Form_Login function. This vulnerability allows attackers to cause a Denial of Service (DoS) via the flag parameter.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-45741	<div>TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a stack overflow in the function setIpv6Cfgr. This vulnerability allows attackers to cause a Denial of Service (DoS) via the relay6to4 parameters.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-45734	<div>TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a stack overflow in the function setUrlFilterRules. This vulnerability allows attackers to cause a Denial of Service (DoS) via the url parameter.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2022-0413	<div>Use After Free in GitHub repository vim/vim prior to 8.2.</div> <div><div>HIGH</div><div>Vector: local</div><div>Created: 2022-01-30</div><div>Updated: 2022-02-04</div></div>
CVE-2021-43859	<div>XStream is an open source java library to serialize objects to XML and back again. Versions prior to 1.4.19 may allow a remote attacker to allocate 100% CPU time on the target system depending on CPU type or parallel execution of such a payload resulting in a denial of service only by manipulating the processed input stream. XStream 1.4.19 monitors and accumulates the time it takes to add elements to collections and throws an exception if a set threshold is exceeded. Users are advised to upgrade as soon as possible. Users unable to upgrade may set the NO_REFERENCE mode to prevent recursion. See GHSA-rmr5-cpv2-vgjf for further details on a workaround if an upgrade is not possible.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>

Source: *NIST*

NIST CVE: Medium

	<div>the settings, this could also lead to a Stored Cross-Site Scripting issue which will be executed in the context of a user viewing any survey</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>
CVE-2021-24919	<div>The Wicked Folders WordPress plugin before 2.8.10 does not sanitise and escape the folder_id parameter before using it in a SQL statement in the wicked_folders_save_sort_order AJAX action, available to any authenticated user. leading to an SQL injection</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>
CVE-2021-45737	<div>TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a stack overflow in the Form_Login function. This vulnerability allows attackers to cause a Denial of Service (DoS) via the Host parameter.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-45736	<div>TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a stack overflow in the function setL2tpServerCfgr. This vulnerability allows attackers to cause a Denial of Service (DoS) via the eip, sip, server parameters.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-45735	<div>TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to use the HTTP protocol for authentication into the admin interface, allowing attackers to intercept user credentials via packet capture software.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-46459	<div>Victor CMS v1.0 was discovered to contain multiple SQL injection vulnerabilities in the component admin/users.php?source=add_user. These vulnerabilities can be exploited through a crafted POST request via the user_name, user_firstname,user_lastname, or user_email parameters.</div> <div><div>HIGH</div><div>Vector: network</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div>
CVE-2021-22815	<div>A CWE-200: Information Exposure vulnerability exists which could cause the troubleshooting archive to be accessed. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU):</div>

CVE-2021-46253

A cross-site scripting (XSS) vulnerability in the Create Post function of **Anchor CMS** v0.12.7 allows attackers to execute arbitrary web scripts or HTML.

MEDIUM	Vector: network	Created: 2022- 02-01	Updated: 2022- 02-04
--------	--------------------	-------------------------	-------------------------

CVE-2021-22810

A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to a delete policy file. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and **Galaxy** 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2

CVE-2021-22813

A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to an edit policy file. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and **Galaxy** 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2

AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)

MEDIUM	Vector: network	Created: 2022- 01-28	Updated: 2022- 02-04
--------	--------------------	-------------------------	-------------------------

AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)			
MEDIUM	Vector: network	Created: 2022-01-28	Updated: 2022-02-04

CVE-2021-22812

A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPP1P2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair			
--	--	--	--

CVE-2021-22811

AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)			
MEDIUM	Vector: network	Created: 2022-01-28	Updated: 2022-02-04

A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause script execution when the request of a privileged account accessing the vulnerable web page is intercepted. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPP1P2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair			
---	--	--	--

IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)

MEDIUM

Vector:
network

Created: 2022-01-28

Updated: 2022-02-04

CVE-2021-22814

A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists which could cause arbitrary script execution when a malicious file is read and displayed. Affected Products: 1-Phase Uninterruptible Power Supply (UPS) using NMC2 including Smart-UPS, Symmetra, and **Galaxy** 3500 with Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.8 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 250/500 (SYPX) Network Management Card 2 (NMC2): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635J (NMC2 AOS V6.9.6 and earlier), 3-Phase Uninterruptible Power Supply (UPS) using NMC2 including Symmetra PX 48/96/100/160 kW UPS (PX2), Symmetra PX 20/40 kW UPS (SY3P), Gutor (SXW, GVX), and Galaxy (GVMTS, GVMSA, GVXTS, GVXSA, G7K, GFC, G9KCHU): AP9630/AP9630CH/AP9630J, AP9631/AP9631CH/AP9631J, AP9635/AP9635CH (NMC2 AOS V6.9.6 and earlier), 1-Phase Uninterruptible Power Supply (UPS) using NMC3 including Smart-UPS, Symmetra, and Galaxy 3500 with Network Management Card 3 (NMC3): AP9640/AP9640J, AP9641/AP9641J, AP9643/AP9643J (NMC3 AOS V1.4.2.1 and earlier), APC Rack Power Distribution Units (PDU) using NMC2 2G Metered/Switched Rack PDUs with embedded NMC2: AP84XX, AP86XX, AP88XX, AP89XX (NMC2 AOS V6.9.6 and earlier), APC Rack Power Distribution Units (PDU) using NMC3 2G Metered/Switched Rack PDUs with embedded NMC3: APDU99xx (NMC3 AOS V1.4.0 and earlier), APC 3-Phase Power Distribution Products using NMC2 Galaxy RPP: GRPPIP2X84 (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) for InfraStruxure 150 kVA PDU with 84 Poles (X84P): PDPB150G6F (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for InfraStruxure 40/60kVA PDU (XPDU) PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10 M,PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular 150/175kVA PDU (XRDP): PDPM150G6F, PDPM150L6F, PDPM175G6H (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for 400 and 500 kVA (PMM): PMM400-ALA, PMM400-ALAX, PMM400-CUB, PMM500-ALA, PMM500-ALAX, PMM500-CUB (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 for Modular PDU (XRDP2G): PDPM72F-5U, PDPM138H-5U, PDPM144F, PDPM138H-R, PDPM277H, PDPM288G6H (NMC2 AOS V6.9.6 and earlier), Rack Automatic Transfer Switches (ATS) Embedded NMC2: Rack Automatic Transfer Switches - AP44XX (ATS4G) (NMC2 AOS V6.9.6 and earlier), Network Management Card 2 (NMC2) Cooling Products: InRow Cooling for series ACRP5xx, ACRP1xx, ACRD5xx, and ACRC5xx SKUs (ACRP2G), InRow Cooling for series ACRC10x SKUs (RC10X2G), InRow Cooling for series ACRD6xx and ACRC6xx SKUs (ACRD2G), InRow Cooling Display for series ACRD3xx (ACRC2G), InRow Cooling for series ACSC1xx SKUs (SC2G), InRow Cooling for series ACRD1xx and ACRD2xx (ACRPTK2G), Ecoflair IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)

MEDIUM

Vector:
network

Created: 2022-01-28

Updated: 2022-02-04

CVE-2021-44414

A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of **reolink RLC-410W** v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. DelUser param is not object. An attacker can send an HTTP request to trigger this vulnerability.

IAEC25/50 Air Economizer Display (EB2G), Uniflair SP UCF0481I, UCF0341I (UNFLRSP), Uniflair LE DX Perimeter Cooling Display for SKUs: IDAV, IDEV, IDWV, IUAV, IUEV, IUWV, IXAV, IXEV, IXWV, LDAV, LDEV, and LDWV (LEDX2G), Refrigerant Distribution Unit: ACDA9xx (RDU) (NMC2 AOS V6.9.6 and earlier), Environmental Monitoring Unit with embedded NMC2 (NB250): NetBotz NBRK0250 (NMC2 AOS V6.9.6 and earlier), and Network Management Card 2 (NMC2): AP9922 Battery Management System (BM4) (NMC2 AOS V6.9.6 and earlier)

MEDIUM

Vector:
network

Created: 2022-01-28

Updated: 2022-02-04

CVE-2021-44413

A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of **reolink RLC-410W** v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. AddUser param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM

Vector:
network

Created: 2022-01-28

Updated: 2022-02-04

CVE-2021-44416

A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of **reolink RLC-410W** v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Disconnect param is not object. An attacker can send an HTTP request to trigger this vulnerability.

	<div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>		<div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44417	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetAlarm param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>	CVE-2021-44406	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetAutoFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44419	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetMdAlarm param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>	CVE-2021-44418	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetMdState param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44412	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. GetRec param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>	CVE-2021-44415	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. ModifyUser param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44411	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. Search param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>	CVE-2021-44405	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. StartZoomFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44407	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. TestEmail param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>	CVE-2021-44408	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. TestFtp param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44409	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. TestWifi param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>	CVE-2021-44410	<div>A denial of service vulnerability exists in the cgiserver.cgi JSON command parser functionality of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a reboot. UpgradePrepare param is not object. An attacker can send an HTTP request to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2022-0286	<div>A flaw was found in the Linux kernel. A null pointer dereference in bond_ipsec_add_sa() may lead to local denial of service.</div> <div><div>MEDIUM</div><div>Vector: local</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div>	CVE-2022-22919	<div>Adenza AxiomSL ControllerView through 10.8.1 allows redirection for SSO login URLs.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-30</div><div>Updated: 2022-02-04</div></div>
CVE-2022-24032	<div>Adenza AxiomSL ControllerView through 10.8.1 is vulnerable to user enumeration. An attacker can identify valid usernames on the platform because a failed login attempt produces a different error message when the username is valid.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-30</div><div>Updated: 2022-02-04</div></div>	CVE-2022-21199	<div>An information disclosure vulnerability exists due to the hardcoded TLS key of reolink RLC-410W v3.0.0.136_20121102. A specially-crafted man-in-the-middle attack can lead to a disclosure of sensitive information. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2021-28096	<div>An issue was discovered in Stormshield SNS before 4.2.3 (when the proxy is used). An attacker can saturate the proxy connection table. This would result in the proxy denying any new connections.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-27</div><div>Updated: 2022-02-04</div></div>	CVE-2020-36056	<div>Beetel 777VR1-DI Hardware Version REV.1.01 Firmware Version V01.00.09_55 was discovered to contain a cross-site scripting (XSS) vulnerability via the Ping diagnostic option.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div>
		CVE-2021-44114	<div>Cross Site Scripting (XSS) vulnerability exists in</div>

CVE-2022-0414	<p>Business Logic Errors in Packagist dolibarr/dolibarr prior to 16.0.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-01-31</div> <div>Updated: 2022-02-04</div> </div>	<p>Sourcecodester Stock Management System in PHP/OOP 1.0, which allows remote malicious users to execute arbitrary remote code execution via create user function.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-01-31</div> <div>Updated: 2022-02-04</div> </div>
CVE-2022-23774	<p>Docker Desktop before 4.4.4 on Windows allows attackers to move arbitrary files.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>	<p>Emlog pro v1.1.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability in the component /admin/configure.php via the parameter footer_info.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-01-31</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-46657	<p>get_sort_by_table in MariaDB before 10.6.2 allows an application crash via certain subquery uses of ORDER BY.</p> <div> <div>MEDIUM</div> <div>Vector: local</div> <div>Created: 2022-01-29</div> <div>Updated: 2022-02-04</div> </div>	<p>gh-ost is a triggerless online schema migration solution for MySQL. Versions prior to 1.1.3 are subject to an arbitrary file read vulnerability. The attacker must have access to the target host or trick an administrator into executing a malicious gh-ost command on a host running gh-ost, plus network access from host running gh-ost to the attack's malicious MySQL server. The ``-database`` parameter does not properly sanitize user input which can lead to arbitrary file reads.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-39021	<p>IBM Guardium Data Encryption (GDE) 5.0.0.2 behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which could facilitate username enumeration. IBM X-Force ID: 213856.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-02-02</div> <div>Updated: 2022-02-04</div> </div>	<p>Improper Access Control in Pypi calibreweb prior to 0.6.16.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-01-30</div> <div>Updated: 2022-02-04</div> </div>
CVE-2022-24197	<p>iText v7.1.17 was discovered to contain a stack-based buffer overflow via the component ByteBuffer.append, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>	<p>iText v7.1.17 was discovered to contain an out-of-bounds exception via the component ARCFOUREncryption.encryptARCFOUR, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>
CVE-2022-24196	<p>iText v7.1.17 was discovered to contain an out-of-memory error via the component readStreamBytesRaw, which allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>	<p>laminas-form is a package for validating and displaying simple and complex forms. When rendering validation error messages via the ``formElementErrors()`` view helper shipped with laminas-form, many messages will contain the submitted value. However, in laminas-form prior to version 3.1.1, the value was not being escaped for HTML contexts, which could potentially lead to a reflected cross-site scripting attack. Versions 3.1.1 and above contain a patch to mitigate the vulnerability. A workaround is available. One may manually place code at the top of a view script where one calls the ``formElementErrors()`` view helper. More information about this workaround is available on the GitHub Security Advisory.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>
CVE-2021-46659	<p>MariaDB before 10.7.2 allows an application crash because it does not recognize that SELECT_LEX::nest_level is local to each VIEW.</p> <div> <div>MEDIUM</div> <div>Vector: local</div> <div>Created: 2022-01-29</div> <div>Updated: 2022-02-04</div> </div>	<p>NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 6.0.0.</p> <div> <div>MEDIUM</div> <div>Vector: local</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>
CVE-2022-23599	<p>Products.ATContentTypes are the core content types for Plone 2.1 - 4.3. Versions of Plone that are dependent on Products.ATContentTypes prior to version 3.0.6 are vulnerable to reflected cross site scripting and open redirect when an attacker can get a compromised version of the image_view_fullscreen page in a cache, for example in Varnish. The technique is known as cache poisoning. Any later visitor can get redirected when clicking on a link on this page. Usually only anonymous users are affected, but this depends on the user's cache settings. Version 3.0.6 of Products.ATContentTypes has been released with a fix. This version works on Plone 5.2, Python 2 only. As a workaround, make sure the image_view_fullscreen page is not stored in the cache. More information about the vulnerability and cvmitigation measures is available in the GitHub Security Advisory.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-01-28</div> <div>Updated: 2022-02-04</div> </div>	<p>Reflected Cross-site scripting (XSS) vulnerability in RosarioSIS 8.2.1 allows attackers to inject arbitrary HTML via the search_term parameter in the modules/Scheduling/Courses.php script.</p> <div> <div>MEDIUM</div> <div>Vector: network</div> <div>Created: 2022-02-01</div> <div>Updated: 2022-02-04</div> </div>

CVE-2021-46658	<p>save_window_function_values in MariaDB before 10.6.3 allows an application crash because of incorrect handling of with_window_func=true for a subquery.</p> <table><tr><td>MEDIUM</td><td>Vector: local</td><td>Created: 2022-01-29</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: local	Created: 2022-01-29	Updated: 2022-02-04	CVE-2021-24937	<p>The Asset CleanUp: Page Speed Booster WordPress plugin before 1.3.8.5 does not escape the wpacu_selected_sub_tab_area parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting issue</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: local	Created: 2022-01-29	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-24983	<p>The Asset CleanUp: Page Speed Booster WordPress plugin before 1.3.8.5 does not sanitise and escape POSTed parameters sent to the wpassetcleanup_fetch_active_plugins_icons AJAX action (available to admin users), leading to a Reflected Cross-Site Scripting issue</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04	CVE-2022-0220	<p>The check_privacy_settings AJAX action of the WordPress GDPR WordPress plugin before 1.9.27, available to both unauthenticated and authenticated users, responds with JSON data without an "application/json" content-type. Since an HTML payload isn't properly escaped, it may be interpreted by a web browser led to this endpoint. Javascript code may be executed on a victim's browser. Due to v1.9.26 adding a CSRF check, the XSS is only exploitable against unauthenticated users (as they all share the same nonce)</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-25063	<p>The Contact Form 7 Skins WordPress plugin through 2.5.0 does not sanitise and escape the tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04	CVE-2021-24944	<p>The Custom Dashboard & Login Page WordPress plugin before 7.0 does not sanitise some of its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-24775	<p>The Document Embedder WordPress plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04	CVE-2021-24868	<p>The Document Embedder WordPress plugin before 1.7.9 contains a AJAX action endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-24926	<p>The Domain Check WordPress plugin before 1.0.17 does not sanitise and escape the domain parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting issue</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04	CVE-2021-24761	<p>The Error Log Viewer WordPress plugin through 1.1.1 does not perform nonce check when deleting a log file and does not have path traversal prevention, which could allow attackers to make a logged in admin delete arbitrary text files on the web server.</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-25097	<p>The LabTools WordPress plugin through 1.0 does not have proper authorisation and CSRF check in place when deleting publications, allowing any authenticated users, such as subscriber to delete arbitrary publication</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04	CVE-2021-24707	<p>The Learning Courses WordPress plugin before 5.0 does not sanitise and escape the Email PDT identity token settings, which could allow high privilege users to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-25092	<p>The Link Library WordPress plugin before 7.2.8 does not have CSRF check when resetting library settings, allowing attackers to make a logged in admin reset arbitrary settings via a CSRF attack</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04	CVE-2021-25091	<p>The Link Library WordPress plugin before 7.2.9 does not sanitise and escape the settingscopy parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2022-23409	<p>The Logs plugin before 3.0.4 for Craft CMS allows remote attackers to read arbitrary files via input to actionStream in Controller.php.</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-01-31</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-01-31	Updated: 2022-02-04	CVE-2021-24975	<p>The NextScripts: Social Networks Auto-Poster WordPress plugin before 4.3.24 does not sanitise and escape logged requests before outputting them in the related admin dashboard, leading to an Unauthenticated Stored Cross-Site Scripting issue</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-01-31	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-25072	<p>The NextScripts: Social Networks Auto-Poster WordPress plugin before 4.3.25 does not have CSRF check in place when deleting items, allowing attacker to make a logged in admin delete arbitrary posts via a CSRF attack</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04	CVE-2021-24900	<p>The Ninja Tables WordPress plugin before 4.1.8 does not sanitise and escape some of its table fields, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed</p> <table><tr><td>MEDIUM</td><td>Vector: network</td><td>Created: 2022-02-01</td><td>Updated: 2022-02-04</td></tr></table>	MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
MEDIUM	Vector: network	Created: 2022-02-01	Updated: 2022-02-04								
CVE-2021-24764	<p>The Perfect Survey WordPress plugin before 1.5.2 does not sanitise and escape multiple parameters (id and filters[session_id] of single_statistics page, type and message of importexport page) before outputting them back in pages/attributes in the admin dashboard, leading</p>	CVE-2021-24765	<p>The Perfect Survey WordPress plugin through 1.5.2 does not validate and escape the X-Forwarded-For header value before outputting it in the statistic page when the Anonymize IP setting of a survey is turned off,</p>								

	<div>to Reflected Cross-Site Scripting issues</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>	<div>leading to a Stored Cross-Site Scripting issue</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>
CVE-2021-24648	<div>The RegistrationMagic WordPress plugin before 5.0.1.9 does not sanitise and escape the <code>rm_search_value</code> parameter before outputting back in an attribute, leading to a Reflected Cross-Site Scripting</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2021-24686</div> <div>The SVG Support WordPress plugin before 2.3.20 does not escape the "CSS Class to target" setting before outputting it in an attribute, which could allow high privilege users to perform Cross-Site Scripting attacks even when the <code>unfiltered_html</code> capability is disallowed.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>
CVE-2021-25089	<div>The UpdraftPlus WordPress Backup Plugin WordPress plugin before 1.16.69 does not sanitise and escape the <code>updraft_restore</code> parameter before outputting it back in the Restore page, leading to a Reflected Cross-Site Scripting</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2021-24934</div> <div>The Visual CSS Style Editor WordPress plugin before 7.5.4 does not sanitise and escape the <code>wyp_page_type</code> parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>
CVE-2021-25085	<div>The WOOF WordPress plugin before 1.2.6.3 does not sanitise and escape the <code>woof_redraw_elements</code> before outputing back in an admin page, leading to a Reflected Cross-Site Scripting</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-02-01</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2021-40042</div> <div>There is a release of invalid pointer vulnerability in some Huawei products, successful exploit may cause the process and service abnormal. Affected product versions include: CloudEngine 12800 V200R019C10SPC800, V200R019C10SPC900; CloudEngine 5800 V200R019C10SPC800, V200R020C00SPC600; CloudEngine 6800 versions V200R019C10SPC800, V200R019C10SPC900, V200R020C00SPC600, V300R020C00SPC200; CloudEngine 7800 V200R019C10SPC800.</div> <div><div>MEDIUM</div><div>Vector: network</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div>
CVE-2021-40033	<div>There is an information exposure vulnerability on several Huawei Products. The vulnerability is due to that the software does not properly protect certain information. Successful exploit could cause information disclosure. Affected product versions include: CloudEngine 12800 V200R005C10SPC800; CloudEngine 5800 V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 V200R005C10SPC800, V200R019C00SPC800.</div> <div><div>MEDIUM</div><div>Vector: local</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2022-22938</div> <div>VMware Workstation (16.x prior to 16.2.2) and Horizon Client for Windows (5.x prior to 5.5.3) contains a denial-of-service vulnerability in the Cortado ThinPrint component. The issue exists in TrueType font parser. A malicious actor with access to a virtual machine or remote desktop may exploit this issue to trigger a denial-of-service condition in the Thinprint service running on the host machine where VMware Workstation or Horizon Client for Windows is installed.</div> <div><div>MEDIUM</div><div>Vector: local</div><div>Created: 2022-01-28</div><div>Updated: 2022-02-04</div></div>
CVE-2022-24130	<div>xterm through Patch 370, when Sixel support is enabled, allows attackers to trigger a buffer overflow in <code>set_sixel</code> in <code>graphics_sixel.c</code> via crafted text.</div> <div><div>MEDIUM</div><div>Vector: local</div><div>Created: 2022-01-31</div><div>Updated: 2022-02-04</div></div>	

Source: *NIST*

NIST CVE: Low

Nothing today

Source: *NIST*

NIST CVE: Unrated

CVE-2021-45268	<div>** DISPUTED ** A Cross Site Request Forgery (CSRF) vulnerability exists in Backdrop CMS 1.20, which allows Remote Attackers to gain Remote Code Execution (RCE) on the Hosting Webserver via uploading a maliciously add-on with crafted PHP file. NOTE: the vendor disputes this because the attack requires a session cookie of a high-privileged authenticated user who is entitled to install arbitrary add-ons.</div> <div><div></div><div>Vector:</div><div>Created:</div><div>Updated:</div></div>	<div>CVE-2021-32732</div> <div>### Impact It's possible to know if a user has or not an account in a wiki related to an email address, and which username(s) is actually tied to that email by forging a request to the Forgot username page. Note that since this page does not have a CSRF check it's quite easy to perform a lot of those requests. ### Patches This issue has been patched in XWiki 12.10.5 and 13.2RC1. Two different patches are provided: - a first one to fix the CSRF problem - a more complex one that now relies on sending an email for the Forgot username process. ### Workarounds It's possible to fix the problem without upgrading by editing the ForgotUsername page in version below 13.x, to use the following code: <code>https://github.com/xwiki/xwiki-platform/blob/69548c0320cbd772540cf4668743e69f879812cf/xwiki-platform-core/xwiki-platform-administration/xwiki-platform-administration-ui/src/main/resources/XWiki/ForgotUsername.xml#L39-L123</code> In version after 13.x it's also possible to edit manually the <code>forgotusername.vm</code> file, but it's really encouraged to upgrade the version here. ### References *</div>
----------------	---	--

	<div>UNRATED</div> <div>unkown</div> <div>2022-02-03</div> <div>2022-02-04</div>	<div>https://jira.xwiki.org/browse/XWIKI-18384 * https://jira.xwiki.org/browse/XWIKI-18408 ### For more information If you have any questions or comments about this advisory: * Open an issue in [Jira XWiki](https://jira.xwiki.org) * Email us at [security ML](mailto:security@xwiki.org)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2021-45429	<div>A Buffer Overflow vulnerability exists in VirusTotal YARA git commit: 605b2edf07ed8eb9a2c61ba22eb2e7c362f47ba7 via yr_set_configuration in yara/libyara/libyara.c, which could cause a Denial of Service.</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	<div>CVE-2021-43635</div> <div>A Cross Site Scripting (XSS) vulnerability exists in Codex before 1.4.0 via Notebook/Page name field, which allows malicious users to execute arbitrary code via a crafted http code in a .json file.</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2021-46398	<div>A Cross-Site Request Forgery (CSRF) vulnerability exists in Filebrowser < 2.18.0 that allows attackers to create a backdoor user with admin privilege and get access to the filesystem via a malicious HTML webpage that is sent to the victim.</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	<div>CVE-2022-22725</div> <div>A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P3 (All versions prior to V30.205)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-22723	<div>A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	<div>CVE-2022-22727</div> <div>A CWE-20: Improper Input Validation vulnerability exists that could allow an unauthenticated attacker to view data, change settings, impact availability of the software, or potentially impact a user?s local machine when the user clicks a specially crafted link. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-22726	<div>A CWE-20: Improper Input Validation vulnerability exists that could allow arbitrary files on the server to be read by authenticated users through a limited operating system service account. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	<div>CVE-2020-7534</div> <div>A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists on the web server used, that could cause a leak of sensitive data or unauthorized actions on the web server during the time the user is logged in. Affected Products: Modicon M340 CPUs: BMXP34 (All Versions), Modicon Quantum CPUs with integrated Ethernet (Copro): 140CPU65 (All Versions), Modicon Premium CPUs with integrated Ethernet (Copro): TSXP57 (All Versions), Modicon M340 ethernet modules: (BMXNOC0401, BMXNOE01, BMXNOR0200H) (All Versions), Modicon Quantum and Premium factory cast communication modules: (140NOE77111, 140NOC78*00, TSXETY5103, TSXETY4103) (All Versions)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-22724	<div>A CWE-400: Uncontrolled Resource Consumption vulnerability exists that could cause a denial of service on ports 80 (HTTP) and 502 (Modbus), when sending a large number of TCP RST or FIN packets to any open TCP port of the PLC. Affected Product: Modicon M340 CPUs: BMXP34 (All Versions)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	<div>CVE-2022-22804</div> <div>A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an authenticated attacker to view data, change settings, or impact availability of the software when the user visits a page containing the injected payload. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-22722	<div>A CWE-798: Use of Hard-coded Credentials vulnerability exists that could result in information disclosure. If an attacker were to obtain the SSH cryptographic key for the device and take active control of the local operational network connected to the product they could potentially observe and manipulate traffic associated with product configuration. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101)</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	<div>CVE-2021-21964</div> <div>A denial of service vulnerability exists in the Modbus configuration functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. Specially-crafted network packets can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability.</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2021-21965	<div>A denial of service vulnerability exists in the SeaMax remote configuration functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. Specially-crafted network packets can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability.</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	<div>CVE-2021-21968</div> <div>A file write vulnerability exists in the OTA update task functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted MQTT payload can lead to arbitrary file overwrite. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.</div> <div>UNRATED</div> <div>Vector:unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>

CVE-2021-21962	<p>A heap-based buffer overflow vulnerability exists in the OTA Update u-download functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A series of specially-crafted MQTT payloads can lead to remote code execution. An attacker must perform a man-in-the-middle attack in order to trigger this vulnerability.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-29218	<p>A local unquoted search path security vulnerability has been identified in HPE Agentless Management Service for Windows version(s): Prior to 1.44.0.0, 10.96.0.0. This vulnerability could be exploited locally by a user with high privileges to execute malware that may lead to a loss of confidentiality, integrity, and availability. HPE has provided software updates to resolve the vulnerability in HPE Agentless Management Service for Windows.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-22150	<p>A memory corruption vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.1.0.52543. A specially-crafted PDF document can trigger an exception which is improperly handled, leaving the engine in an invalid state, which can lead to memory corruption and arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-21959	<p>A misconfiguration exists in the MQTTS functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. This misconfiguration significantly simplifies a man-in-the-middle attack, which directly leads to control of device functionality.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-24249	<p>A Null Pointer Dereference vulnerability exists in GPAC 1.1.0 via the xtra_box_write function in /box_code_base.c, which causes a Denial of Service. This vulnerability was fixed in commit 71f9871.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-38130	<p>A potential Information leakage vulnerability has been identified in versions of Micro Focus Voltage SecureMail Mail Relay prior to 7.3.0.1. The vulnerability could be exploited to create an information leakage attack.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-29219	<p>A potential local buffer overflow vulnerability has been identified in HPE FlexNetwork 5130 EL Switch Series version: Prior to 5130_EI_7.10.R3507P02. HPE has made the following software update to resolve the vulnerability in HPE FlexNetwork 5130 EL Switch Series version 5130_EL_7.10.R3507P02.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23330	<p>A remote code execution (RCE) vulnerability in HelloWorldAddonController.java of jpress v4.2.0 allows attackers to execute arbitrary code via a crafted JAR package.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23805	<p>A security out-of-bounds read information disclosure vulnerability in Trend Micro Worry-Free Business Security Server could allow a local attacker to send garbage data to a specific named pipe and crash the server. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-24260	<p>A SQL injection vulnerability in Voipmonitor GUI before v24.96 allows attackers to escalate privileges to the Administrator level.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-21960	<p>A stack-based buffer overflow vulnerability exists in both the LLMNR functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted network packet can lead to remote code execution. An attacker can send a malicious packet to trigger this vulnerability.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23947	<p>A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon DCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23946	<p>A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon GCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-21961	<p>A stack-based buffer overflow vulnerability exists in the NBNS functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted network packet can lead to remote code execution. An attacker can send a malicious packet to trigger this vulnerability.</p> <table> <tr> <td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr> </table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-4154	<p>A use-after-free flaw was found in cgroup1_parse_param in kernel/cgroup/cgroup-v1.c in the Linux kernel's cgroup v1 parser. A local attacker with a user privilege could cause a privilege escalation by exploiting the fsconfig syscall parameter leading to a container breakout and a denial of service on the system.</p> <table> <tr> <td></td><td>Vector:</td><td>Created:</td><td>Updated:</td></tr> </table>		Vector:	Created:	Updated:	CVE-2021-40420	<p>A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.1.0.52543. A specially-crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.</p> <table> <tr> <td></td><td>Vector:</td><td>Created: 2022-02-</td><td>Updated: 2022-02-</td></tr> </table>		Vector:	Created: 2022-02-	Updated: 2022-02-
	Vector:	Created:	Updated:								
	Vector:	Created: 2022-02-	Updated: 2022-02-								

	UNRATED	unknown	2022-02-04	2022-02-04
--	---------	---------	------------	------------

CVE-2021-40401	A use-after-free vulnerability exists in the RS-274X aperture definition tokenization functionality of Gerbv 2.7.0 and dev (commit b5f1eacd) and Gerbv forked 2.7.1. A specially-crafted gerber file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2022-23329	A vulnerability in \${"freemarker.template.utility.Execute"?new()} of UJCMS Jspxcms v10.2.0 allows attackers to execute arbitrary commands via uploading malicious files.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2021-29394	Account Hijacking in /northstar/Admin/changePassword.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote authenticated users to change the password of any targeted user accounts via lack of proper authorization in the user-controlled "userID" parameter of the HTTP POST request.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2020-12891	AMD Radeon Software may be vulnerable to DLL Hijacking through path variable. An unprivileged user may be able to drop its malicious DLL file in any location which is in path environment variable.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2022-0317	An improper input validation vulnerability in go-attestation before 0.3.3 allows local users to provide a maliciously-formed Quote over no/some PCRs, causing AKPublic.Verify to succeed despite the inconsistency. Subsequent use of the same set of PCR values in Eventlog.Verify lacks the authentication performed by quote verification, meaning a local attacker could couple this vulnerability with a maliciously-crafted TCG log in Eventlog.Verify to spoof events in the TCG log, hence defeating remotely-attested measured-boot. We recommend upgrading to Version 0.4.0 or above.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2021-40403	An information disclosure vulnerability exists in the pick-and-place rotation parsing functionality of Gerbv 2.7.0 and dev (commit b5f1eacd), and Gerbv forked 2.8.0. A specially-crafted pick-and-place file can exploit the missing initialization of a structure to leak memory contents. An attacker can provide a malicious file to trigger this vulnerability.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2022-24448	An issue was discovered in fs/nfs/dir.c in the Linux kernel before 5.16.5. If an application sets the O_DIRECTORY flag, and tries to open a regular file, nfs_atomic_open() performs a regular lookup. If a regular file is found, ENOTDIR should occur, but the server instead returns uninitialized data in the file descriptor.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2021-21970	An out-of-bounds write vulnerability exists in the HandleSeaCloudMessage functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. The HandleIncomingSeaCloudMessage function uses at [3] the json_object_get_string to populate the p_name global variable. The p_name is only 0x80 bytes long, and the total			
----------------	---	--	--	--

UNRATED	unknown	04	04
---------	---------	----	----

CVE-2022-0487	A use-after-free vulnerability was found in rtsx_usb_ms_drv_remove in drivers/memstick/host/rtsx_usb_ms.c in memstick in the Linux kernel. In this flaw, a local attacker with a user privilege may impact system Confidentiality. This flaw affects kernel versions prior to 5.14 rc1.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2022-0264	A vulnerability was found in the Linux kernel's eBPF verifier when handling internal data structures. Internal memory locations could be returned to userspace. A local attacker with the permissions to insert eBPF code to the kernel can use this to leak internal kernel memory details defeating some of the exploit mitigations in place for the kernel. This flaws affects kernel versions < v5.16-rc6			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2020-12966	AMD EPYC(tm) Processors contain an information disclosure vulnerability in the Secure Encrypted Virtualization with Encrypted State (SEV-ES) and Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP). A local authenticated attacker could potentially exploit this vulnerability leading to leaking guest data by the malicious hypervisor.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2021-32036	An authenticated user without any specific authorizations may be able to repeatedly invoke the features command where at a high volume may lead to resource depletion or generate high lock contention. This may result in denial of service and in rare cases could result in id field collisions.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2022-24259	An incorrect check in the component cdr.php of Voipmonitor GUI before v24.96 allows unauthenticated attackers to escalate privileges via a crafted request.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2021-21963	An information disclosure vulnerability exists in the Web Server functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted man-in-the-middle attack can lead to a disclosure of sensitive information. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2022-23316	An issue was discovered in taoCMS v3.0.2. There is an arbitrary file read vulnerability that can read any files via admin.php? action=file&ctrl=download&path=../1.txt.			
	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04

CVE-2021-21969	An out-of-bounds write vulnerability exists in the HandleSeaCloudMessage functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. The HandleIncomingSeaCloudMessage function uses at [4] the json_object_get_string to populate the p_payload global variable. The p_payload is only 0x100 bytes long,			
----------------	--	--	--	--

	<p>MQTT message could be up to 0x201 bytes. Because the function <code>json_object_get_string</code> will fill str based on the length of the json's value and not the actual str size, this would result in a possible out-of-bounds write.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04		<p>and the total MQTT message could be up to 0x201 bytes. Because the function <code>json_object_get_string</code> will fill str based on the length of the json's value and not the actual str size, this would result in a possible out-of-bounds write.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-21971	<p>An out-of-bounds write vulnerability exists in the <code>URL_decode</code> functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted MQTT payload can lead to an out-of-bounds write. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-36152	<p>Apache Gobblin trusts all certificates used for LDAP connections in Gobblin-as-a-Service. This affects versions <= 0.15.0. Users should update to version 0.16.0 which addresses this issue.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-24348	<p>Argo CD before 2.1.9 and 2.2.x before 2.2.4 allows directory traversal related to Helm charts because of an error in <code>helmTemplate</code> in <code>repository.go</code>. For example, an attacker may be able to discover credentials stored in a YAML file.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-0227	<p>Business Logic Errors in GitHub repository <code>silverstripe/silverstripe-framework</code> prior to 4.10.1.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-22689	<p>CA Harvest Software Change Manager versions 13.0.3, 13.0.4, 14.0.0, and 14.0.1, contain a vulnerability in the CSV export functionality, due to insufficient input validation, that can allow a privileged user to potentially execute arbitrary code or commands.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-29397	<p>Cleartext Transmission of Sensitive Information in <code>/northstar/Admin/login.jsp</code> in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote local user to intercept users credentials transmitted in cleartext over HTTP.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23980	<p>Cross-Site Scripting (XSS) vulnerability discovered in Yasr - Yet Another Stars Rating WordPress plugin (versions <= 2.9.9), vulnerable at parameter 'source'.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-46457	<p>D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function <code>ChgSambaUserSettings</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>samba_name</code> parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-46452	<p>D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function <code>SetNetworkTomographySettings</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>tomography_ping_address</code>, <code>tomography_ping_number</code>, <code>tomography_ping_size</code>, <code>tomography_ping_timeout</code>, and <code>tomography_ping_ttl</code> parameters.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-46453	<p>D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function <code>SetStaticRouteSettings</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>staticroute_list</code> parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-46455	<p>D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function <code>SetStationSettings</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>station_access_enable</code> parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-46456	<p>D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function <code>SetWlanACLSettings</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>wl(0).(0)_maclist</code> parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-46454	<p>D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function <code>SetWlanApCliSettings</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>ApCliKeyStr</code> parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-46228	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function <code>httpd_debug.asp</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>time</code> parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-46233	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function <code>msp_info.htm</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>cmd</code> parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-46227	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function <code>proxy_client.asp</code>. This vulnerability allows attackers to execute arbitrary commands via the <code>proxy_srv</code>, <code>proxy_srvport</code>, <code>proxy_lanip</code>, <code>proxy_lanport</code> parameters.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								

CVE-2021-46230	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function upgrade_filter. This vulnerability allows attackers to execute arbitrary commands via the path and time parameters.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-46231	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function urlrd_opt.asp. This vulnerability allows attackers to execute arbitrary commands via the url_en parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-46229	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function usb_paswd.asp. This vulnerability allows attackers to execute arbitrary commands via the name parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-46232	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function version_upgrade.asp. This vulnerability allows attackers to execute arbitrary commands via the path parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-46226	<p>D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function wget_test.asp. This vulnerability allows attackers to execute arbitrary commands via the url parameter.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-44882	<p>D-Link device DIR_878_FW1.30B08_Hotfix_02 was discovered to contain a command injection vulnerability in the twsystem function. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-45998	<p>D-Link device DIR_882 DIR_882_FW1.30B06_Hotfix_02 was discovered to contain a command injection vulnerability in the LocalIPAddress parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-44881	<p>D-Link device DIR_882 DIR_882_FW1.30B06_Hotfix_02 was discovered to contain a command injection vulnerability in the twsystem function. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-44880	<p>D-Link devices DIR_878 DIR_878_FW1.30B08_Hotfix_02 and DIR_882 DIR_882_FW1.30B06_Hotfix_02 were discovered to contain a command injection vulnerability in the system function. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-29398	<p>Directory traversal in /northstar/Common/NorthFileManager/fileManagerObjects.jsp Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to browse and list the directories across the entire filesystem of the host of the web application.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2021-29395	<p>Directory travesal in /northstar/filemanager/download.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to download arbitrary files, including JSP source code, across the filesystem of the host of the web application.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23379	<p>Emlog v6.0 was discovered to contain a SQL injection vulnerability via the \$TagID parameter of getblogidsfromtagid().</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23600	<p>fleet is an open source device management, built on osquery. Versions prior to 4.9.1 expose a limited ability to spoof SAML authentication with missing audience verification. This impacts deployments using SAML SSO in two specific cases: 1. A malicious or compromised Service Provider (SP) could reuse the SAML response to log into Fleet as a user -- only if the user has an account with the same email in Fleet, and the user signs into the malicious SP via SAML SSO from the same Identity Provider (IdP) configured with Fleet. 2. A user with an account in Fleet could reuse a SAML response intended for another SP to log into Fleet. This is only a concern if the user is blocked from Fleet in the IdP, but continues to have an account in Fleet. If the user is blocked from the IdP entirely, this cannot be exploited. Fleet 4.9.1 resolves this issue. Users unable to upgrade should: Reduce the length of sessions on your IdP to reduce the window for malicious re-use, Limit the amount of SAML Service Providers/Applications used by user accounts with access to Fleet, and When removing access to Fleet in the IdP, delete the Fleet user from Fleet as well.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04	CVE-2021-38960	<p>IBM OPENBMC OP920, OP930, and OP940 could allow an unauthenticated user to obtain sensitive information. IBM X-Force ID: 212047.</p> <table><tr><td>UNRATED</td><td>Vector: unknown</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknown	Created: 2022-02-04	Updated: 2022-02-04								

CVE-2021-44978	<p>iCMS <= 8.0.0 allows users to add and render a comtom template, which has a SSTI vulnerability which causes remote code execution.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2021-22285	<p>Improper Handling of Exceptional Conditions, Improper Check for Unusual or Exceptional Conditions vulnerability in the ABB SPIET800 and PNI800 module that allows an attacker to cause the denial of service or make the module unresponsive.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2021-22286	<p>Improper Input Validation vulnerability in the ABB SPIET800 and PNI800 module allows an attacker to cause the denial of service or make the module unresponsive.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2021-22288	<p>Improper Input Validation vulnerability in the ABB SPIET800 and PNI800 module allows an attacker to cause the denial of service or make the module unresponsive.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2022-23913	<p>In Apache ActiveMQ Artemis prior to 2.20.0 or 2.19.1, an attacker could partially disrupt availability (DoS) through uncontrolled resource consumption of memory.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2021-36151	<p>In Apache Gobblin, the Hadoop token is written to a temp file that is visible to all local users on Unix-like systems. This affects versions <= 0.15.0. Users should update to version 0.16.0 which addresses this issue.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2021-44977	<p>In iCMS <=8.0.0, a directory traversal vulnerability allows an attacker to read arbitrary files.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2021-46320	<p>In OpenZeppelin <=v4.4.0, initializer functions that are invoked separate from contract creation (the most prominent example being minimal proxies) may be reentered if they make an untrusted non-view external call. Once an initializer has finished running it can never be re-executed. However, an exception put in place to support multiple inheritance made reentrancy possible, breaking the expectation that there is a single execution.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2021-44983	<p>In taocms 3.0.1 after logging in to the background, there is an Arbitrary file download vulnerability at the File Management column.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2021-44886	<p>In Zammad 5.0.2, agents can configure "out of office" periods and substitute persons. If the substitute persons didn't have the same permissions as the original agent, they could receive ticket notifications for tickets that they have no access to.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2021-22284	<p>Incorrect Permission Assignment for Critical Resource vulnerability in OPC Server for AC 800M allows an attacker to execute arbitrary code in the node running the AC800M OPC Server.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2022-23611	<p>iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize image file paths leading to OS level command injection. This issue has been patched in commit cdc448b. Users are advised to upgrade.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2022-23609	<p>iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize user input used to remove files leading to file deletion only limited by the process permissions. Users are advised to upgrade as soon as possible.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2022-0484	<p>Lack of validation of URLs causes Mirantis Container Cloud Lens Extension before v3.1.1 to open external programs other than the default browser to perform sign on to a new cluster. An attacker could host a webserver which serves a malicious Mirantis Container Cloud configuration file and induce the victim to add a new cluster via its URL. This issue affects: Mirantis Mirantis Container Cloud Lens Extension v3 versions prior to v3.1.1.</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2021-44206	<p>Local privilege escalation due to DLL hijacking vulnerability in Acronis Media Builder service. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2021-44205	<p>Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2022-24113	<p>Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>	CVE-2022-24114	<p>Local privilege escalation due to race condition on application startup. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287</p> <p>UNRATED Vector: unknown Created: 2022-02-04 Updated: 2022-02-04</p>
CVE-2022-24115	<p>Local privilege escalation due to unrestricted loading of unsigned libraries. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605,</p>	CVE-2021-44204	<p>Local privilege escalation via named pipe due to improper access control checks. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows)</p>

	<div>Acronis True Image 2021 (macOS) before build 39287</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>before build 39612, Acronis True Image 2021 (Windows) before build 39287</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44900	<div>Micro-Star International (MSI) App Player <= 4.280.1.6309 is vulnerable to multiple Privilege Escalation (LPE/EoP) vulnerabilities in the NTIOLib_X64.sys and BstkJrv_msi2.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2021-44899</div> <div>Micro-Star International (MSI) Center <= 1.0.31.0 is vulnerable to multiple Privilege Escalation vulnerabilities in the atidgllk.sys, atilk64.sys, MODAPI.sys, NTIOLib.sys, NTIOLib_X64.sys, WinRing0.sys, WinRing0x64.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-44903	<div>Micro-Star International (MSI) Center Pro <= 2.0.16.0 is vulnerable to multiple Privilege Escalation (LPE/EoP) vulnerabilities in the atidgllk.sys, atilk64.sys, MODAPI.sys, NTIOLib.sys, NTIOLib_X64.sys, WinRing0.sys, WinRing0x64.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2021-44901</div> <div>Micro-Star International (MSI) Dragon Center <= 2.0.116.0 is vulnerable to multiple Privilege Escalation (LPE/EoP) vulnerabilities in the atidgllk.sys, atilk64.sys, MODAPI.sys, NTIOLib.sys, NTIOLib_X64.sys, WinRing0.sys, WinRing0x64.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-4043	<div>NULL Pointer Dereference in GitHub repository gpac/gpac prior to 1.1.0.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2022-0481</div> <div>NULL Pointer Dereference in Homebrew mruby prior to 3.2.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-45408	<div>Open Redirect vulnerability exists in SeedDMS 6.0.15 in out.Login.php, which llows remote malicious users to redirect users to malicious sites using the "referuri" parameter.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2021-46671</div> <div>options.c in atftp before 0.7.5 reads past the end of an array, and consequently discloses server-side /etc/group data to a remote client.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2021-29393	<div>Remote Code Execution in cominput.jsp and comoutput.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to inject and execute arbitrary system commands via the unsanitized user-controlled "command" and "commandvalues" parameters.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2021-29396</div> <div>Systemic Insecure Permissions in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to use various functionalities without authentication.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2022-24150	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function formSetSafeWanWebMan. This vulnerability allows attackers to execute arbitrary commands via the remoteIp parameter.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2022-24148</div> <div>Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function mDMZSetCfg. This vulnerability allows attackers to execute arbitrary commands via the dmzIp parameter.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2022-24144	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function WanParameterSetting. This vulnerability allows attackers to execute arbitrary commands via the gateway, dns1, and dns2 parameters.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2022-24161</div> <div>Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function GetParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the mac parameter.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2022-24155	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function setSchedWifi. This vulnerability allows attackers to cause a Denial of Service (DoS) via the schedStartTime and schedEndTime parameters.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>	<div>CVE-2022-24143</div> <div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>
CVE-2022-24153	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formAddMacfilterRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter.</div> <div><div></div><div>Vector:</div><div>Created:</div><div>Updated:</div></div>	<div>CVE-2022-24160</div> <div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetDeviceName. This vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter.</div> <div><div>UNRATED</div><div>Vector: unknown</div><div>Created: 2022-02-04</div><div>Updated: 2022-02-04</div></div>

	<div>UNRATED</div> <div>unkown</div> <div>2022-02-04</div> <div>2022-02-04</div>		
CVE-2022-24142	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetFirewallCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the firewallEn parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24157	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetMacFilterCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceList parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24159	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetPPTPServer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the startIp and endIp parameters.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24146	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetQosBand. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24154	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetRebootTimer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the rebootTime parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24156	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24145	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formWifiBasicSet. This vulnerability allows attackers to cause a Denial of Service (DoS) via the security and security_5g parameters.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24147	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromAdvSetMacMtuWan. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wanMTU, wanSpeed, cloneType, mac, and serviceName parameters.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24158	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetIpMacBind. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24152	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetRouteStatic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24163	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24151	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetWifiGusetBasic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the shareSpeed parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24149	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetWirelessRepeat. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wpapsk_crypto parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24162	<div>Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24167	<div>Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetDMZ. This vulnerability allows attackers to execute arbitrary commands via the dmzHost1 parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2022-24168	<div>Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpGroup. This vulnerability allows attackers to execute arbitrary commands via the IPGroupStartIP and IPGroupEndIP parameters.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24170	<div>Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpSecTunnel. This vulnerability allows attackers to execute arbitrary commands via the IPsecLocalNet and IPsecRemoteNet parameters.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>	CVE-2021-45987	<div>Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetNetCheckTools. This vulnerability allows attackers to execute arbitrary commands via the hostName parameter.</div> <div>UNRATED</div> <div>Vector: unkown</div> <div>Created: 2022-02-04</div> <div>Updated: 2022-02-04</div>
CVE-2022-24171	<div>Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to</div>		

contain a command injection vulnerability in the function formSetPppoeServer. This vulnerability allows attackers to execute arbitrary commands via the pppoeServerIP, pppoeServerStartIP, and pppoeServerEndIP parameters.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45986

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetUSBShareInfo. This vulnerability allows attackers to execute arbitrary commands via the usbOrdinaryUserName parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2022-24172

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddDhcpBindRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the addDhcpRules parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45991

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddVpnUsers. This vulnerability allows attackers to cause a Denial of Service (DoS) via the vpnUsers parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2022-24169

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindAdd. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRule parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45996

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetPortMapping. This vulnerability allows attackers to cause a Denial of Service (DoS) via the portMappingServer, portMappingProtocol, portMappingWan, porMappingtInternal, and portMappingExternal parameters.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45992

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetQvlanList. This vulnerability allows attackers to cause a Denial of Service (DoS) via the qvlanName parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2022-24166

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the manualTime parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45989

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function guestWifiRuleRefresh. This vulnerability allows attackers to cause a Denial of Service (DoS) via the qosGuestUpstream and qosGuestDownstream parameters.

CVE-2022-24165

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetQvlanList. This vulnerability allows attackers to execute arbitrary commands via the qvlanIP parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45990

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function uploadPicture. This vulnerability allows attackers to execute arbitrary commands via the pic_name parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45988

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddDnsForward. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsForwardRule parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45994

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formDelDhcpRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the delDhcpIndex parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45993

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindModify. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRuleIP and IPMacBindRuleMac parameters.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45997

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetPortMapping. This vulnerability allows attackers to cause a Denial of Service (DoS) via the portMappingServer, portMappingProtocol, portMappingWan, porMappingtInternal, and portMappingExternal parameters.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2021-45995

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetStaticRoute. This vulnerability allows attackers to cause a Denial of Service (DoS) via the staticRouteNet, staticRouteMask, and staticRouteGateway parameters.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2022-24164

Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsHijackRule parameter.

UNRATED

Vector: unknown

Created: 2022-02-04

Updated: 2022-02-04

CVE-2022-23590

Tensorflow is an Open Source Machine Learning Framework. A `GraphDef` from a TensorFlow `SavedModel` can be maliciously altered to cause a TensorFlow process to crash due to encountering a `StatusOr` value that is an error and forcibly extracting the value from it. We have patched the issue in multiple **GitHub** commits and these will be included in TensorFlow 2.8.0 and TensorFlow 2.7.1, as both are affected.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23582

Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a ``SavedModel`` such that ``TensorByteSize`` would trigger ``CHECK`` failures. ``TensorShape`` constructor throws a ``CHECK`` -fail if shape is partial or has a number of elements that would overflow the size of an ``int``. The ``PartialTensorShape`` constructor instead does not cause a ``CHECK``-abort if the shape is partial, which is exactly what this function needs to be able to return ``-1``. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23586

Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a ``SavedModel`` such that assertions in ``function.cc`` would be falsified and crash the **Python** interpreter. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23584

Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a use after free behavior when decoding PNG images. After ``png::CommonFreeDecode(&decode)`` gets called, the values of ``decode.width`` and ``decode.height`` are in an unspecified state. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23561

Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite **model** that would cause a write outside of bounds of an array in TFLite. In fact, the attacker can override the linked list used by the memory allocator. This can be leveraged for an arbitrary write primitive under certain conditions. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23559

Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite **model** that would cause an integer overflow in embedding lookup operations. Both ``embedding_size`` and ``lookup_size`` are products of values provided by the user. Hence, a malicious user could trigger overflows in the multiplication. In certain scenarios, this can then result in heap OOB read/write. Users are advised to upgrade to a patched version.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23565

Tensorflow is an Open Source Machine Learning Framework. An attacker can trigger denial of service via assertion failure by altering a ``SavedModel`` on disk such that ``AttrDef``s of some operation are duplicated. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23583

Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a ``SavedModel`` such that any binary op would trigger ``CHECK`` failures. This occurs when the **protobuf** part corresponding to the tensor arguments is modified such that the ``dtype`` no longer matches the ``dtype`` expected by the op. In that case, calling the templated binary operator for the binary op would receive corrupted data, due to the type confusion involved. If ``Tin`` and ``Tout`` don't match the type of data in ``out`` and ``input_*`` tensors then ``flat<*>`` would interpret it wrongly. In most cases, this would be a silent failure, but we have noticed scenarios where this results in a ``CHECK`` crash, hence a denial of service. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23588

Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a ``SavedModel`` such that Grappler optimizer would attempt to build a tensor using a reference ``dtype``. This would result in a crash due to a ``CHECK``-fail in the ``Tensor`` constructor as reference types are not allowed. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23560

Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite **model** that would allow limited reads and writes outside of arrays in TFLite. This exploits missing validation in the conversion from sparse tensors to dense tensors. The fix is included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. Users are advised to upgrade as soon as possible.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23558

Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite **model** that would cause an integer overflow in ``TfLiteIntArrayCreate``. The ``TfLiteIntArrayGetSizeInBytes`` returns an ``int`` instead of a ``size_t``. An attacker can control model inputs such that ``computed_size`` overflows the size of ``int`` datatype. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23557

Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite **model** that would trigger a division by zero in ``BiasAndClamp`` implementation. There is no check that the ``bias_size`` is non zero. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
---------	----------------	---------------------	---------------------

CVE-2022-23580

Tensorflow is an Open Source Machine Learning Framework. During shape inference, TensorFlow can allocate a large vector based on a value from a tensor controlled by the user. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
--	----------------	---------------------	---------------------

	UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
--	---------	-------------------	------------------------	------------------------

CVE-2022-23578

Tensorflow is an Open Source Machine Learning Framework. If a graph node is invalid, TensorFlow can leak memory in the implementation of ``ImmutableExecutorState::Initialize``. Here, we set ``item->kernel`` to ``nullptr`` but it is a simple ``OpKernel*`` pointer so the memory that was previously allocated to it would leak. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-23566

Tensorflow is an Open Source Machine Learning Framework. TensorFlow is vulnerable to a heap OOB write in ``Grappler``. The ``set_output`` function writes to an array at the specified index. Hence, this gives a malicious user a write primitive. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-23591

Tensorflow is an Open Source Machine Learning Framework. The ``GraphDef`` format in TensorFlow does not allow self recursive functions. The **runtime** assumes that this invariant is satisfied. However, a ``GraphDef`` containing a fragment such as the following can be consumed when loading a ``SavedModel``. This would result in a stack overflow during execution as resolving each ``NodeDef`` means resolving the function itself and its nodes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-23581

Tensorflow is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a ``SavedModel`` such that ``IsSimplifiableReshape`` would trigger ``CHECK`` failures. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-23573

Tensorflow is an Open Source Machine Learning Framework. The implementation of ``AssignOp`` can result in copying uninitialized data to a new tensor. This later results in undefined behavior. The implementation has a check that the left hand side of the assignment is initialized (to minimize number of allocations), but does not check that the right hand side is also initialized. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-23576

Tensorflow is an Open Source Machine Learning Framework. The implementation of ``OpLevelCostEstimator::CalculateOutputSize`` is vulnerable to an integer overflow if an attacker can create an operation which would involve tensors with large enough number of elements. We can have a large enough number

UNRATED	unknown	04	04
---------	---------	----	----

CVE-2022-23563

Tensorflow is an Open Source Machine Learning Framework. In multiple places, TensorFlow uses ``tempfile.mktemp`` to create temporary files. While this is acceptable in testing, in utilities and libraries it is dangerous as a different process can create the file between the check for the filename in ``mktemp`` and the actual creation of the file by a subsequent operation (a TOC/TOU type of weakness). In several instances, TensorFlow was supposed to actually create a temporary directory instead of a file. This logic bug is hidden away by the ``mktemp`` function usage. We have patched the issue in several commits, replacing ``mktemp`` with the safer ``mkstemp``/``mkdtemp`` functions, according to the usage pattern. Users are advised to upgrade as soon as possible.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2022-23592

Tensorflow is an Open Source Machine Learning Framework. TensorFlow's type inference can cause a heap out of bounds read as the bounds checking is done in a ``DCHECK`` (which is a no-op during production). An attacker can control the ``input_idx`` variable such that ``ix`` would be larger than the number of values in ``node_t.args``. The fix will be included in TensorFlow 2.8.0. This is the only affected version.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2022-23593

Tensorflow is an Open Source Machine Learning Framework. The ``simplifyBroadcast`` function in the MLIR-TFRT infrastructure in TensorFlow is vulnerable to a segfault (hence, denial of service), if called with scalar shapes. If all shapes are scalar, then ``maxRank`` is 0, so we build an empty ``SmallVector``. The fix will be included in TensorFlow 2.8.0. This is the only affected version.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2022-23579

Tensorflow is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a ``SavedModel`` such that ``SafeToRemoveIdentity`` would trigger ``CHECK`` failures. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2022-23577

Tensorflow is an Open Source Machine Learning Framework. The implementation of ``GetInitOp`` is vulnerable to a crash caused by dereferencing a null pointer. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2022-23575

Tensorflow is an Open Source Machine Learning Framework. The implementation of ``OpLevelCostEstimator::CalculateTensorSize`` is vulnerable to an integer overflow if an attacker can create an operation which would involve a tensor with large enough number

	<p>of dimensions in <code>output.shape.dim()</code> or just a small number of dimensions being large enough to cause an overflow in the multiplication. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04		<p>of elements. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23562	<p>Tensorflow is an Open Source Machine Learning Framework. The implementation of <code>`Range`</code> suffers from integer overflows. These can trigger undefined behavior or, in some scenarios, extremely large allocations. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23594	<p>Tensorflow is an Open Source Machine Learning Framework. The TFG dialect of TensorFlow (MLIR) makes several assumptions about the incoming <code>`GraphDef`</code> before converting it to the MLIR-based dialect. If an attacker changes the <code>`SavedModel`</code> format on disk to invalidate these assumptions and the <code>`GraphDef`</code> is then converted to MLIR-based IR then they can cause a crash in the Python interpreter. Under certain scenarios, heap OOB read/writes are possible. These issues have been discovered via fuzzing and it is possible that more weaknesses exist. We will patch them as they are discovered.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23574	<p>Tensorflow is an Open Source Machine Learning Framework. There is a typo in TensorFlow's <code>`SpecializeType`</code> which results in heap OOB read/write. Due to a typo, <code>`arg`</code> is initialized to the <code>`i`</code>th mutable argument in a loop where the loop index is <code>`j`</code>. Hence it is possible to assign to <code>`arg`</code> from outside the vector of arguments. Since this is a mutable proto value, it allows both read and write to outside of bounds data. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23589	<p>Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler component of TensorFlow can trigger a null pointer dereference. There are 2 places where this can occur, for the same malicious alteration of a <code>`SavedModel`</code> file (fixing the first one would trigger the same dereference in the second place). First, during constant folding, the <code>`GraphDef`</code> might not have the required nodes for the binary operation. If a node is missing, the corresposning <code>`mul *child`</code> would be null, and the dereference in the subsequent line would be incorrect. We have a similar issue during <code>`IsIdentityConsumingSwitch`</code>. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23587	<p>Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler component of TensorFlow is vulnerable to an integer overflow during cost estimation for crop and resize. Since the cropping parameters are user controlled, a malicious person can trigger undefined behavior. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23572	<p>Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, TensorFlow can fail to specialize a type during shape inference. This case is covered by the <code>`DCHECK`</code> function however, <code>`DCHECK`</code> is a no-op in production builds and an assertion failure in debug builds. In the first case execution proceeds to the <code>`ValueOrDie`</code> line. This results in an assertion failure as <code>`ret`</code> contains an error <code>`Status`</code>, not a value. In the second case we also get a crash due to the assertion failure. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23595	<p>Tensorflow is an Open Source Machine Learning Framework. When building an XLA compilation cache, if default settings are used, TensorFlow triggers a null pointer dereference. In the default scenario, all devices are allowed, so <code>`flr->config_proto`</code> is <code>`nullptr`</code>. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23564	<p>Tensorflow is an Open Source Machine Learning Framework. When decoding a resource handle tensor from protobuf, a TensorFlow process can encounter cases where a <code>`CHECK`</code> assertion is invalidated based on user controlled arguments. This allows attackers to cause denial of services in TensorFlow processes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23571	<p>Tensorflow is an Open Source Machine Learning Framework. When decoding a tensor from protobuf, a TensorFlow process can encounter cases where a <code>`CHECK`</code> assertion is invalidated based on user controlled arguments, if the tensors have an invalid <code>`dtype`</code> and 0 elements or an invalid shape. This allows attackers to cause denial of services in TensorFlow processes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04	CVE-2022-23570	<p>Tensorflow is an Open Source Machine Learning Framework. When decoding a tensor from protobuf, TensorFlow might do a null-dereference if attributes of some mutable arguments to some operations are missing from the proto. This is guarded by a <code>`DCHECK`</code>. However, <code>`DCHECK`</code> is a no-op in production builds and an assertion failure in debug builds. In the first case execution proceeds to the dereferencing of the null pointer, whereas in the second case it results in a crash due to the assertion failure. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range.</p> <table><tr><td>UNRATED</td><td>Vector: unknwn</td><td>Created: 2022-02-04</td><td>Updated: 2022-02-04</td></tr></table>	UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
UNRATED	Vector: unknwn	Created: 2022-02-04	Updated: 2022-02-04								
CVE-2022-23585	<p>Tensorflow is an Open Source Machine</p>										

Learning Framework. When decoding PNG images TensorFlow can produce a memory leak if the image is invalid. After calling ``png::CommonInitDecode(..., &decode)``, the ``decode`` value contains allocated buffers which can only be freed by calling ``png::CommonFreeDecode(&decode)``. However, several error case in the function implementation invoke the ``OP_REQUIRES`` macro which immediately terminates the execution of the function, without allowing for the memory free to occur. The fix will be included in TensorFlow 2.8.0. We will also cherry-pick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-22987

The affected product has a hardcoded private key available inside the project folder, which may allow an attacker to achieve Web Server login and perform further actions.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2022-0365

The affected product is vulnerable to an authenticated OS command injection, which may allow an attacker to inject and execute arbitrary shell commands as the Admin (root) user.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-24262

The config restore function of **Voipmonitor** GUI before v24.96 does not properly check files sent as restore archives, allowing remote attackers to execute arbitrary commands via a crafted file in the web root.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2022-0381

The Embed **Swagger WordPress** plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping/sanitization and validation via the url parameter found in the `~/swagger-iframe.php` file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 1.0.0.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-0380

The Fotobook **WordPress** plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping and the use of `$ _SERVER['PHP_SELF']` found in the `~/options-fotobook.php` file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 3.2.3.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2021-28503

The impact of this vulnerability is that Arista's EOS eAPI may skip re-evaluating user credentials when certificate based authentication is used, which allows remote attackers to access the device via eAPI.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-24129

The OIDC OP plugin before 3.0.4 for **Shibboleth Identity Provider** allows server-side request forgery (SSRF) due to insufficient restriction of the request_uri parameter. This allows attackers to **interact** with arbitrary third-party HTTP services.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2021-23507

The package object-path-set before 1.0.2 are vulnerable to Prototype Pollution via the `setPath` method, as it allows an attacker to **merge** object prototypes into it. *Note:* This vulnerability derives from an incomplete fix in <https://security.snyk.io/vuln/SNYK-JS-OBJECTPATHSET-607908>

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2022-0218

The WP HTML **Mail WordPress** plugin is vulnerable to unauthorized access which allows unauthenticated attackers to retrieve and modify theme settings due to a missing capability check on the `/themesettings` REST-API endpoint found in the `~/includes/class-template-designer.php` file, in versions up to and including 3.0.9. This makes it possible for attackers with no privileges to execute the endpoint and add malicious JavaScript to a vulnerable WordPress site.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2018-25029

The Z-Wave specification requires that S2 security can be downgraded to S0 or other less secure protocols, allowing an attacker within radio range during pairing to downgrade and then exploit a different vulnerability (CVE-2013-20003) to intercept and spoof traffic.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2021-23497

This affects the package `@strikeentco/set` before 1.0.2. It allows an attacker to cause a denial of service and may lead to remote code execution. **Note:** This vulnerability derives from an incomplete fix in <https://security.snyk.io/vuln/SNYK-JS-STRIKEENTCOSET-1038821>

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2021-23470

This affects the package `putil-merge` before 3.8.0. The `merge()` function does not check the values passed into the argument. An attacker can supply a malicious value by adjusting the value to include the constructor property. Note: This vulnerability derives from an incomplete fix in <https://security.snyk.io/vuln/SNYK-JS-PUTILMERGE-1317077>

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	------------------------	------------------------

CVE-2021-44246

Totolink devices A3100R v4.1.2cu.5050_B20200504, A830R v5.9c.4729_B20191112, and A720R v4.1.5cu.470_B20200911 were discovered to contain a stack overflow in the function `setNoticeCfg`. This vulnerability allows attackers to cause a Denial of Service (DoS) via the `IpTo` parameter.

UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04
---------	-------------------	---------------------	---------------------

CVE-2021-44247

Totolink devices A3100R v4.1.2cu.5050_B20200504, A830R v5.9c.4729_B20191112, and A720R v4.1.5cu.470_B20200911 were discovered to contain command injection vulnerability in the function `setNoticeCfg`. This vulnerability allows attackers to execute arbitrary commands via the `IpFrom` parameter.

UNRATED	Vector:	Created:	Updated:
---------	---------	----------	----------

CVE-2022-23614

Twig is an open source template language for PHP. When in a sandbox mode, the ``arrow`` parameter of the ``sort`` filter must be a closure to avoid attackers being able to run arbitrary PHP functions. In affected versions this constraint was not properly enforced and could lead to code injection of arbitrary PHP code. Patched versions now disallow calling non Closure in the ``sort`` filter as is the case for some other filters. Users are advised to upgrade.

UNRATED	Vector:	Created: 2022-02-	Updated: 2022-02-
---------	---------	-------------------	-------------------

		unkown	2022-02-04	2022-02-04			unkown	04	04
CVE-2021-44779	Unauthenticated SQL Injection (SQLi) vulnerability discovered in [GWA] AutoResponder WordPress plugin (versions <= 2.3), vulnerable at (&listid). No patched version available, plugin closed.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	
CVE-2022-22939	VMware Cloud Foundation contains an information disclosure vulnerability due to logging of credentials in plain-text within multiple log files on the SDDC Manager. A malicious actor with root access on VMware Cloud Foundation SDDC Manager may be able to view credentials in plaintext within one or more log files.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	
CVE-2022-23605	Wire webapp is a web client for the wire messaging protocol. In versions prior to 2022-01-27-production.0 expired ephemeral messages were not reliably removed from local chat history of Wire Webapp. In versions before 2022-01-27-production.0 ephemeral messages and assets might still be accessible through the local search functionality. Any attempt to view one of these message in the chat view will then trigger the deletion. This issue only affects locally stored messages. On premise instances of wire-webapp need to be updated to 2022-01-27-production.0, so that their users are no longer affected. There are no known workarounds for this issue.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	
CVE-2021-43841	XWiki is a generic wiki platform offering runtime services for applications built on top of it. When using default XWiki configuration, it's possible for an attacker to upload an SVG containing a script executed when executing the download action on the file. This problem has been patched so that the default configuration doesn't allow to display the SVG files in the browser. Users are advised to update or to disallow uploads of SVG files.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	
CVE-2022-0472	Unrestricted Upload of File with Dangerous Type in Packagist jsdecena/laracom prior to v2.0.9.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	
CVE-2020-12965	When combined with specific software sequences, AMD CPUs may transiently execute non-canonical loads and store using only the lower 48 address bits potentially resulting in data leakage.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	
CVE-2021-43145	With certain LDAP configurations, Zammad 5.0.1 was found to be vulnerable to unauthorized access with existing user accounts.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	
CVE-2013-20003	Z-Wave devices from Sierra Designs (circa 2013) and Silicon Labs (using S0 security) may use a known, shared network key of all zeros, allowing an attacker within radio range to spoof Z-Wave traffic.				UNRATED	Vector: unkown	Created: 2022-02-04	Updated: 2022-02-04	

Source: *Hybrid Analysis*

Top malicious files									
100% Threat score	Photoshop_Set-Up (.) exe				100% Threat score	svchost (.) exe			
100% Threat score	Setup (.) exe				100% Threat score	TPY4514 (.) exe			
100% Threat score	RK-1579611692 (.) xlsb				100% Threat score	ç»åœ°æ±,ç”ÝăŽ¸æž‘ă...è¹æµ¸è¹• (.) exe			
100% Threat score	mpserver-installer (.) exe				100% Threat score	XBOOT (.) exe			
100% Threat score	43279133 (.) exe				100% Threat score	0203 (.) dotm			
100% Threat score	2022-04-02_1621 (.) xls				97% Threat score	Setup (.) exe			
93% Threat score	4d80bb9d0dc53583ceb20e9af95f25f1ceeb33370f15c77ec6179e5fb76ec6b7 (.) xlsx				89% Threat score	YOWA9 (.) 20-By (.) SamMods (.) 58 (.) apk			
85% Threat score	PL23XX-M_LogoDriver_Setup_v400_20211229 (.) exe				81% Threat score	update_flshtplayerx64 (.) vbs			

77% Threat score	minehut_op_exploit (.) exe	75% Threat score	setup (.) exe
75% Threat score	KOS_Setup (.) exe		

Source: *Hybrid Analysis*

Top malicious URL

100% Threat score	http://182 (.) 121 (.) 162 (.) 93:51703/Mozi (.) m	100% Threat score	http://636500 (.) selcdn (.) ru/
100% Threat score	http://www (.) usyd (.) edu (.) au (.) weblogon (.) xyz/	100% Threat score	http://www (.) ezproxy1 (.) library (.) usyd (.) edu (.) au (.) weblogon (.) xyz/
100% Threat score	http://ms-work (.) com-info (.) store/	100% Threat score	http://59 (.) 58 (.) 117 (.) 29:42928/i
100% Threat score	http://78 (.) 161 (.) 137 (.) 58:33876/Mozi (.) m	100% Threat score	http://221 (.) 14 (.) 204 (.) 47:44833/Mozi (.) m
100% Threat score	http://182 (.) 56 (.) 238 (.) 113:37044/Mozi (.) m	100% Threat score	http://171 (.) 104 (.) 127 (.) 171:44734/Mozi (.) a
90% Threat score	http://nobelie (.) com/	90% Threat score	http://dddn (.) com (.) vn/
90% Threat score	https://freeextremecams (.) com/top10	89% Threat score	http://www (.) averagesocialite (.) com/
86% Threat score	https://194 (.) 67 (.) 109 (.) 164:zB6OZj6F0zYfSQ	82% Threat score	http://www (.) northpoleroute (.) com/newimage (.) asp?imageid=yedaww2043349717&type=0&resid=125576781
82% Threat score	http://www (.) northpoleroute (.) com/newimage (.) asp?imageid=xyaawc1606366848&type=0&resid=172185390	82% Threat score	https://cumshots (.) com/t5/index (.) php?t=newslide
82% Threat score	https://familysimulator (.) com/t4/index (.) php?t=xxxgames-newslide	82% Threat score	https://familysimulator (.) com/t4/index (.) php?t=porngames-160x600banner
82% Threat score	http://electricalrs (.) com/gardenedci (.) php?utm_source=c97&%3Butm_content=74ab956	80% Threat score	http://636500 (.) selcdn (.) ru/scans3/bbdef085359361/covid_form (.) htm
77% Threat score	https://cartoonporn (.) games/	77% Threat score	https://www (.) bk8vietnam (.) com/register?affid=16567
77% Threat score	http://hoadonhoaphat (.) com/	77% Threat score	http://www (.) 1edu (.) in/safa/nima/link (.) php?M=241&%3Bamp%3BN=6&%3Bamp%3BL=2&%3Bamp%3BF=H
74% Threat score	http://vietnamba (.) org (.) vn/	73% Threat score	http://gramerly (.) com/
72% Threat score	http://ms-work (.) com-info (.) store/home/up (.) xn--php?id=%5B%5D-i020bn36ch97b0rj	72% Threat score	http://duset (.) marketing/

Source: *SpamHaus*

Top spamming countries

 #1 United States of America	 #2 China
 #3 Russian Federation	 #4 Mexico
 #5 Dominican Republic	 #6 India
 #7 Saudi Arabia	 #8 Japan
#9 Brazil	#10 Korea, Republic of



Source: [SpamHaus](#)

Top spammers

	#1 Canadian Pharmacy A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.		#2 PredictLabs / Sphere Digital This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.
	#3 Hosting Response / Michael Boehm Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.		#4 Mint Global Marketing / Adgenics / Cabo Networks Florida affiliate spammers and bulletproof spam hosts
	#5 RetroCubes Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.		#6 Michael Persaud Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.
	#7 Cyber World Internet Services/ e-Insites Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.		#8 RR Media A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.
	#9 Kobeni Solutions High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US FTC in 2014.		

Source: [SpamHaus](#)

Top countries with botnet

	#1 China		#2 India
	#3 Thailand		#4 Indonesia
	#5 United States of America		#6 Algeria
	#7 Brazil		#8 Viet Nam
	#9 Pakistan		#10 Iran (Islamic Republic of)

Source: [SpamHaus](#)

Top phishing countries

	#1 United States		#2 Russia
	#3 Netherlands		#4 India
	#5 Germany		#6 France
	#7 Hong Kong		#8 United Kingdom
	#9 Singapore		#10 Ireland

