Your Security Rabbits report for February 03, 2022

Hot topics

Update Chrome now

Google has released Chrome versions 98.0.4758.80/81/82 for Windows and 98.0.4758.80 for Mac and Linux that fix some serious security flaws, allowing an attacker to take control of the system.

Access to the bug details are restricted until a majority of users are updated with a fix.

It is recommended to patch Chrome quickly.

News

ZDNet | security RSS

3D printed guns, underground markets, bomb manuals: police crackdown continues
Europol has now turned its attention to freely-available bomb guides published online.

Security Affairs

Antlion APT group used a custom backdoor that allowed them to fly under the radar for months
A China-linked APT group tracked as Antlion used a custom backdoor called xPack that was undetected for months. A China-linked APT group tracked as Antlion is using a custom backdoor called xPack in attacks aimed at financial organizations and manufacturing companies, Symantec researchers reported. The backdoor was undetected for at least 18 months in a [...] The post Antlion APT group used a custom backdoor that allowed them to fly under the radar for months appeared first on Security Affairs.

Security Affairs

Cisco fixes critical flaws in its Small Business Routers
Cisco released security patches to address multiple flaws in its Small Business RV160, RV260, RV340, and RV345 series routers. Cisco announced patches for multiple issue affecting its Small Business RV160, RV260, RV340, and RV345 series routers. Some of the bugs fixed by the IT giant could lead to the execution of arbitrary code with root [...] The post Cisco fixes critical flaws in its Small Business Routers appeared first on Security Affairs.

Cyware News - Latest Cyber News

Common authentication and authorization vulnerabilities (and how to avoid them)
In the OWASP Top 10 for 2021, broken access control is the number 1 cause of web application security issues, with no fewer than 34 weaknesses grouped under this category.

The Hacker News

Critical Flaws Discovered in Cisco Small Business RV Series Routers
Cisco has patched multiple critical security vulnerabilities impacting its RV Series routers that could be weaponized to elevate privileges and execute arbitrary code on affected systems, while also warning of the existence of proof-of-concept (PoC) exploit code targeting some of these bugs. Three of the 15 flaws, tracked as CVE-2022-20699, CVE-2022-20700, and CVE-2022-20707, carry the highest

Cyware News - Latest Cyber News

Cybercriminals Seek Ransomware Payments and Settlements
Cybercriminals are doing their homework. Cybercriminals making ransomware demands want to know if you have insurance because they know they are more likely to get paid if you do.

Cyware News - Latest Cyber News

Hackers Abuse Vulnerability in Smart Contracts Cryptocurrency Platform Wormhole
The attack took place earlier today and impacted Wormhole Portal, a web-based application--also known as a blockchain "bridge"--that allows users to convert one form of cryptocurrency into another.

CyberScoop

Hackers stole more than $320 million in cryptocurrency from DeFi platform Wormhole
A hacker stole $320 million worth of Ethereum cryptocurrency from decentralized finance platform Wormhole on Wednesday. The attack is the largest against the cryptocurrency industry so far in 2022 and one of the top hacks of the industry to date. As of Thursday morning, all of the stolen funds were "restored," the trading platform was back up, and an incident report was coming soon, according to tweets by the company. The vulnerability used by the attacker had been fixed, Wormhole said late Wednesday. The platform allows users to send Ethereum and Solana cryptocurrencies across two different

IT Security Guru

9 out of 10 Security Leaders Warn of Skills Shortage
Despite business backing and a recruitment push, new research suggests most tech security decision-makers are struggling to address the skilled professional shortage. Stott and May, a global cybersecurity recruitment firm has joined forces with venture investor Forgepoint Capital to compose the Cyber Security in Focus. Responses from cybersecurity directors, security operations directors and VPs of product [...] The post 9 out of 10 Security Leaders Warn of Skills Shortage appeared first on IT Security Guru.

Cyware News - Latest Cyber News

BotenaGo Source Code Leaked - What does it Mean?
AT&T experts unearthed the new BotenaGo botnet, which leaked on GitHub last year. It could target 33 exploits affecting nearly 2 million routers and IoT devices. Experts also discovered several hacking tools--from several sources--in the same GitHub repository. The leak of such ready-to-use source code of BotenaGo could result in the further explosion of new malware variants.

Cyware News - Latest Cyber News

Civicom Exposed More Than 100,000 Files Containing 8TB of Personal and Client Data
A New York City-based company known for providing audio, web conferencing, and market research services was found exposing a trove of personal and sensitive data to its clients.

Threatpost

Critical Cisco Bugs Open VPN Routers to Cyberattacks
The company's RV line of small-business routers contains 15 different security vulnerabilities that could enable everything from RCE to corporate network access and denial-of-service - and many have exploits circulating.

Cyware News - Latest Cyber News

Cybercriminals Bypass MFA, Stealing Browser Sessions Using MiTM Phishing Kits
Threat actors are using phish kits that leverage transparent reverse proxy, which enables them to man-in-the-middle (MitM) a browser session and steal credentials and session cookies in real-time.

Security Affairs

Exclusive interview with the Powerful Greek Army (PGA) hacker group
Six years ago the Powerful Greek Army (PGA) appeared in the threat landscape. After a long breach the hacker collective is back. I have interviewed them in exclusive ... enjoy it! Tell me about your hacker team, which is the motivation behind the attacks? We have many motivations and reasons. First of all, we started [...] The post Exclusive interview with the Powerful Greek Army (PGA) hacker group appeared first on Security Affairs.

IT Security Guru

Hackers steal $326 million from blockchain platform Wormhole
Hackers have exploited a vulnerability in the Wormhole cross-chain crypto platform to the tune of $326 million in cryptocurrency. Wormhole is a platform enabling users to transfer cryptocurrency across different blockchains. It locks the original token in a smart contract and mints a wrapped version of the stored token that is trans. Avalanche, Oasis, Binance [...] The post Hackers steal $326 million from blockchain platform Wormhole appeared first on IT Security Guru.

Krebs on Security

How Phishers Are Slinking Their Links Into LinkedIn
If you received a link to LinkedIn.com via email, SMS or instant message, would you click it? Spammers, phishers and other ne'er-do-wells are hoping you will, because they've long taken advantage of a marketing feature on the business networking site which lets them create a LinkedIn.com link that bounces your browser to other websites, such as phishing pages that mimic top online brands (but chiefly Linkedin's parent firm Microsoft).

blockchains. A preliminary analysis of the attack by blockchain security firm CertiK shared with Cybe[...]

The Hacker News

How SSPM Simplifies Your SOC2 SaaS Security Posture Audit

An accountant and a security expert walk into a bar... SOC2 is no joke. Whether you're a publicly held or private company, you are probably considering going through a Service Organization Controls (SOC) audit. For publicly held companies, these reports are required by the Securities and Exchange Commission (SEC) and executed by a Certified Public Accountant (CPA). However, customers often ask

IT Security Guru

KP snacks hit with ransomware attack

KP Snacks, purveyor of iconic British snacks such as Skips and Butterkist, has been hit with a ransomware attack threatening to impact deliveries at least until the end of March. The company announced that Conti, an incredibly effective Russian-speaking group, is behind the attack. As is typical for the gang, they stole data in a [...] The post KP snacks hit with ransomware attack appeared first on IT Security Guru.

Threatpost

Low-Detection Phishing Kits Increasingly Bypass MFA

A growing class of phishing kits - transparent reverse proxy kits - are being used to get past multi-factor authentication using MiTM tactics.

The Hacker News

New SEO Poisoning Campaign Distributing Trojanized Versions of Popular Software

An ongoing search engine optimization (SEO) poisoning attack campaign has been observed abusing trust in legitimate software utilities to trick users into downloading BATLOADER malware on compromised machines. "The threat actor used 'free productivity apps installation' or 'free software development tools installation' themes as SEO keywords to lure victims to a compromised website and to

The Hacker News

New Wave of Cyber Attacks Target Palestine with Political Bait and Malware

Cybersecurity researchers have turned the spotlight on a new wave of offensive cyberattacks targeting Palestinian activists and entities starting around October 2021 using politically-themed phishing emails and decoy documents. The intrusions are part of what Cisco Talos calls a longstanding espionage and information theft campaign undertaken by the Arid Viper hacking group using a Delphi-based

Security Affairs

Oil terminals in Europe's biggest ports hit by a cyberattack

A cyber attack hit the oil terminals of some of the biggest European ports impacting their operations. Some of the major oil terminals in Western Europe's biggest ports have been targeted with a cyberattack. Threat actors have hit multiple oil facilities in Belgium's ports, including Antwerp, which is the second biggest port in Europe after [...] The post Oil terminals in Europe's biggest ports hit by a cyberattack appeared first on Security Affairs.

Threatpost

PowerPoint Files Abused to Take Over Computers

Attackers are using socially engineered emails with .ppam file attachments that hide malware that can rewrite Windows registry settings on targeted machines.

Naked Security

S3 Ep68: Bugs, scams, privacy ...and fonts?! [Podcast + Transcript]

Latest episode - listen now!

Cyware News - Latest Cyber News

Target shares its own web skimming detection tool Merry Maker with the world

The new open-source tool Merry Maker from Target simulates online browsing and shopping to identify malicious code meant to steal payment card information on retailers' websites.

Blog â€“ Flashpoint

The Death of an ISIS Leader; ISIS Attacks, January 2022: Key Trends, Statistics, and Geographic Analysis

The following research is based on information gathered by Flashpoint analysts and data collections. For December's report, click here. The Death of ISIS Leader Abu Ibrahim al-Hashimi al-Qurayshi Early in the morning of February 3, 2022, U.S. special operations forces carried out a raid near Atmeh in northwestern Syria's Idlib Province that led to the [...] The post The Death of an ISIS Leader; ISIS Attacks, January 2022: Key Trends, Statistics, and Geographic Analysis appeared first on Flashpoint.

Cyware News - Latest Cyber News

Trend Micro Patches Vulnerabilities in Hybrid Cloud Security Products

The vulnerabilities are tracked as CVE-2022-23119 and CVE-2022-23120, and they impact Deep Security and Cloud One workload security solutions, specifically the Linux agent component.

Threatpost

Wormhole Crypto Platform: 'Funds Are Safe' After $314M Heist

The popular bridge, which connects Ethereum, Solana blockchain & more, was shelled out by it's-not-saying. Wormhole is trying to negotiate with the attacker.

Cyware News - Latest Cyber News

KP Snacks Faces Manufacturing Disruptions Following Ransomware Attack

Responding to a SecurityWeek inquiry, KP Snacks said it began investigating the attack soon after enacting its cybersecurity response plan. However, the situation hasn't been resolved as of yet.

Threatpost

Kronos Still Dragging Itself Back From Ransomware Hell

And customers including Tesla, PepsiCo and NYC transit workers are filing lawsuits over the "real pain in the rear end" of manual inputting, inaccurate wages & more.

Cyware News - Latest Cyber News

MacOS Malware UpdateAgent Grows Increasingly Malicious

The macOS malware, dubbed UpdateAgent, was found propagating for almost 14 months. It started circulating around November or December 2020 as a basic infostealer.

The Hacker News

New Variant of UpdateAgent Malware Infects Mac Computers with Adware

Microsoft on Wednesday shed light on a previously undocumented Mac trojan that it said has undergone several iterations since its first appearance in September 2020, effectively granting it an "increasing progression of sophisticated capabilities." The company's Microsoft 365 Defender Threat Intelligence Team dubbed the new malware family "UpdateAgent," charting its evolution from a barebones

IT Security Guru

Obrela acquires Encode to become one of Europe's largest MDR players

Obrela Security Industries, a leading provider of security analytics and cyber risk management services, has announced the acquisition of Encode, a Security Analytics and Response Orchestration provider. The move establishes Obrela as one of the largest cybersecurity and Managed Detection and Response (MDR) players in the EMEA. George Patsis, CEO of Obrela said, "Our acquisition [...] The post Obrela acquires Encode to become one of Europe's largest MDR players appeared first on IT Security Guru.

Cyware News - Latest Cyber News

OT Data Stolen by Ransomware Gangs can Fuel Other Sophisticated Attacks, Reveals Research

In 2021, Mandiant Threat Intelligence observed that over 1,300 organizations in the critical and industrial sectors were impacted by ransomware attacks.

Cyware News - Latest Cyber News

Ransomware Often Hits Industrial Systems, With Significant Impact: Survey

In a new survey, 80% of respondents admitted that their organization had experienced a ransomware attack within the past year, and nearly half said the incident had impacted their ICS/OT environment.

CyberScoop

State Department sounds alarm over Red Cross breach

The U.S. State Department said the hack of the International Committee of the Red Cross last month was a "dangerous development" that has harmed the organization's family re-unification mission. The commentary from Foggy Bottom comes in response to a Jan. 19 announcement from the Red Cross that a cyberattack compromised personal data for more than half a million people from at least 60 Red Cross and associated Red Crescent national organizations across the globe. "Targeting the Red Cross and Red Crescent Movement's sensitive and confidential data is a dangerous development," said Ned Price, a spokesman for the State Department. "It has real consequences: this cyber incident has harmed the gl[...]

Cyware News - Latest Cyber News

Tennessee Community College Suffers Ransomware Attack

The college's main database and credit card payment systems were not involved, and no data from them was accessed by unauthorized users, said the board, which oversees the state's community colleges.

Security Affairs

Trend Micro fixed 2 flaws in Hybrid Cloud Security products

Trend Micro recently addressed two high-severity flaws affecting some of its hybrid cloud security products. Trend Micro released security updates to fix two high-severity vulnerabilities, tracked as CVE-2022-23119 and CVE-2022-23120, affecting some of its hybrid cloud security products. The vulnerabilities affect Deep Security and Cloud One workload security solutions. The flaws were reported by the cybersecurity [...] The post Trend Micro fixed 2 flaws in Hybrid Cloud Security products appeared first on Security Affairs.

Cyware News - Latest Cyber News

US State Department offers $10M for information on Iranian election interference

The Department is offering a reward for information on two Iranian hackers who allegedly participated in state-sponsored cyber operations designed to interfere with the 2020 presidential election.

Security Affairs

Wormhole cryptocurrency platform hacked, crooks stole $326 million, the second-biggest hack of a DeFi platform

Threat actors have stolen $325 million in cryptocurrency leveraging a bug in the Wormhole communication bridge. Wormhole, one of the most popular bridges that links the Ethereum and Solana blockchains, lost about $325 million in an attack that took place on Wednesday. This is the second-biggest hack of a DeFi

platform ever, just after the $600 [...] The post Wormhole cryptocurrency platform hacked, crooks stole $326 million, the second-biggest hack of a DeFi platform appeared first on Security Affairs.

Twitter

Cyber Advising: CVE-2021-45897: SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows remote code execution. PoC

CyCatz: #cycatz #bugbountytips #bugbounty CVE-2021-45897 SuiteCRM Privilege Escalation #RCE #appsec More..

Ptrace Security GmbH: PoC for CVE-2021-45897 #Pentesting #CyberSecurity #Infosec

blueblue: GitHub - manuelz120/CVE-2021-45897: PoC for CVE-2021-45897 -

Necio: manuelz120/CVE-2021-45897: PoC for CVE-2021-45897 #Infosec #cybersecurity #security

Robo Shadow Alerts: Potentially Critical CVE Detected! CVE-2021-45897 Description: SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows remote code execution.... CVSS: 9.37 #suitecrm #suitecrm #CVE #CyberSecurity #DataBreach

RedPacket Security: Reolink RLC-410W command execution | CVE-2021-40409 -

Remotely Alerts: Severity: | An OS command injection vulnerability ex... | CVE-2021-40409 | Link for more:

RedPacket Security: Reolink RLC-410W command execution | CVE-2021-40408 -

Remotely Alerts: Severity: | An OS command injection vulnerability ex... | CVE-2021-40408 | Link for more:

RedPacket Security: Reolink RLC-410W command execution | CVE-2021-40407 -

Remotely Alerts: Severity: | An OS command injection vulnerability ex... | CVE-2021-40407 | Link for more:

Source: NIST

NIST CVE: Critical

CVE-2021-22820
A CWE-614 Insufficient Session Expiration vulnerability exists that could allow an attacker to maintain an unauthorized access over a hijacked session to the charger station web server even after the legitimate user account holder has changed his password. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)

CRITICAL Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40404
An authentication bypass vulnerability exists in the cgiserver.cgi Login functionality of **reolink RLC-410W** v3.0.0.136_20121102. A specially-crafted HTTP request can lead to authentication bypass. An attacker can send an HTTP request to trigger this vulnerability.

CRITICAL Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40407
An OS command injection vulnerability exists in the device network settings functionality of **reolink RLC-410W** v3.0.0.136_20121102. At [1] or [2], based on DDNS type, the ddns->domain variable, that has the value of the domain parameter provided through the SetDdns API, is not validated properly. This would lead to an OS command injection. An attacker can send an HTTP request to trigger this vulnerability.

CRITICAL Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40409
An OS command injection vulnerability exists in the device network settings functionality of **reolink RLC-410W** v3.0.0.136_20121102. At [1] or [2], based on DDNS type, the ddns->password variable, that has the value of the password parameter provided through the SetDdns API, is not validated properly. This would lead to an OS command injection.

CRITICAL Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40408
An OS command injection vulnerability exists in the device network settings functionality of **reolink RLC-410W** v3.0.0.136_20121102. At [1] or [2], based on DDNS type, the ddns->username variable, that has the value of the userName parameter provided through the SetDdns API, is not validated properly. This would lead to an OS command injection.

CRITICAL Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-21817
NVIDIA Omniverse **Launcher** contains a Cross-Origin Resource Sharing (CORS) vulnerability which can allow an unprivileged remote attacker, if they can get user to browse malicious site, to acquire access tokens allowing them to access **resources** in other security domains, which may lead to code execution, escalation of privileges, and impact to confidentiality and integrity.

CRITICAL Vector: network Created: 2022-02-02 Updated: 2022-02-03

CVE-2021-45897
SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows remote code execution.

CRITICAL Vector: network Created: 2022-01-28 Updated: 2022-02-03

Source: NIST

NIST CVE: High

CVE-2021-22827
A CWE-20: Improper Input Validation vulnerability exists that could cause arbitrary code execution when the user visits a page containing the injected payload. This CVE is unique from CVE-2021-22826. Affected Product: EcoStruxure? **Power** Monitoring Expert 9.0 and prior versions

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-22826
A CWE-20: Improper Input Validation vulnerability exists that could cause arbitrary code execution when the user visits a page containing the injected payload. This CVE is unique from CVE-2021-22827. Affected Product: EcoStruxure? **Power** Monitoring Expert 9.0 and prior versions

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-22825
A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could allow an attacker to access the system with elevated privileges when a privileged account clicks on a malicious URL that compromises the security token. Affected Products: AP7xxxx and AP8xxx with NMC2 (V6.9.6 or earlier), AP7xxx and AP8xxx with NMC3 (V1.1.0.3 or earlier), and APDU9xxx with NMC3 (V1.0.0.28 or earlier)

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-22818
A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow an attacker to gain unauthorized access to the charging station **web interface** by performing brute force attacks. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-22816

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a Denial of Service of the RTU when receiving a specially crafted request over Modbus, and the RTU is configured as a Modbus server. Affected Products: SCADAPack 312E, 313E, 314E, 330E, 333E, 334E, 337E, 350E and 357E RTUs with firmware V8.18.1 and prior

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40423

A denial of service vulnerability exists in the cgiserver.cgi API command parser functionality of **Reolink RLC-410W** v3.0.0.136_20121102. A specially-crafted series of HTTP requests can lead to denial of service. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44379

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. SetAutoMaint param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44378

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. SetEnc param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44377

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. SetImage param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44372

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. SetLocalLink param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44368

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. SetNetPort param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44381

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. SetPowerLed param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44380

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. SetTime param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40406

A denial of service vulnerability exists in the cgiserver.cgi session creation functionality of **reolink RLC-410W** v3.0.0.136_20121102. A specially-crafted HTTP request can lead to prevent users from logging in. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40389

A privilege escalation vulnerability exists in the installation of **Advantech** DeviceOn/iEdge Server 1.0.2. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40397

A privilege escalation vulnerability exists in the installation of **Advantech** WISE-PaaS/OTA Server 3.0.9. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40416

An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of **reolink RLC-410W** v3.0.0.136_20121102. All the Get APIs that are not included in cgi_check_ability are already executable by any logged-in users. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-22821

A CWE-918 Server-Side Request Forgery (SSRF) vulnerability exists that could cause the station web server to forward requests to unintended network targets when crafted malicious parameters are submitted to the charging station web server. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44373

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. SetAutoFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44371

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. SetEmail param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44370

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. SetFtp param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44376

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. SetIsp param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44374

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. SetMask param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44369

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. SetNtp param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44384

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. SetPtzTattern param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44367

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. SetUpnp param is not object. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40388

A privilege escalation vulnerability exists in **Advantech** SQ **Manager Server** 1.0.6. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40396

A privilege escalation vulnerability exists in the installation of **Advantech** DeviceOn/iService 1.1.7. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-21944

A **UNIX** Symbolic Link (Symlink) Following vulnerability in the **systemd** service file for watchman of **openSUSE Backports** SLE-15-SP3, Factory allows local attackers to escalate to root. This issue affects: openSUSE Backports SLE-15-SP3 watchman versions prior to 4.9.0. openSUSE Factory watchman versions prior to 4.9.0-9.1.

HIGH Vector: local Created: 2022-01-26 Updated: 2022-02-03

CVE-2021-40414

An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of **reolink RLC-410W** v3.0.0.136_20121102. The SetMdAlarm API sets the movement detection parameters, giving the ability to set the sensitivity of the camera per a range of hours, and which of the camera **spaces** to ignore when considering movement detection. Because in cgi_check_ability the SetMdAlarm API does not have a specific case, the user permission will default to 7. This will give non-administrative users the possibility to change the movement detection parameters.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40413 An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of **reolink RLC-410W** v3.0.0.136_20121102. The UpgradePrepare is the API that checks if a provided filename identifies a new version of the RLC-410W firmware. If the version is new, it would be possible, allegedly, to later on perform the Upgrade. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-21236 An information disclosure vulnerability exists due to a web server misconfiguration in the **Reolink RLC-410W** v3.0.0.136_20121102. A specially-crafted HTTP request can lead to a disclosure of sensitive information. An attacker can send an HTTP request to trigger this vulnerability.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40410 An OS command injection vulnerability exists in the device network settings functionality of **reolink RLC-410W** v3.0.0.136_20121102. At [4] the dns_data->dns1 variable, that has the value of the dns1 parameter provided through the SetLocal API, is not validated properly. This would lead to an OS command injection.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40411 An OS command injection vulnerability exists in the device network settings functionality of **reolink RLC-410W** v3.0.0.136_20121102. At [6] the dns_data->dns2 variable, that has the value of the dns2 parameter provided through the SetLocalLink API, is not validated properly. This would lead to an OS command injection.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40412 An OScommand injection vulnerability exists in the device network settings functionality of **reolink RLC-410W** v3.0.0.136_20121102. At [8] the devname variable, that has the value of the name parameter provided through the SetDevName API, is not validated properly. This would lead to an OS command injection.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-41766 **Apache Karaf** allows monitoring of applications and the **Java runtime** by using the Java Management Extensions (JMX). JMX is a Java RMI based technology that relies on Java serialized objects for client server communication. Whereas the default JMX implementation is hardened against unauthenticated deserialization attacks, the implementation used by Apache Karaf is not protected against this kind of attack. The impact of Java deserialization vulnerabilities strongly depends on the classes that are available within the targets class path. Generally speaking, deserialization of untrusted data does always represent a high security risk and should be prevented. The risk is low as, by default, Karaf uses a limited set of classes in the JMX server class path. It depends of system scoped classes (e.g. jar in the lib folder).

HIGH Vector: network Created: 2022-01-26 Updated: 2022-02-03

CVE-2021-40339 Configuration vulnerability in **Hitachi** Energy LinkOne application due to the lack of HTTP Headers, allows an attacker that manages to exploit this vulnerability to retrieve sensitive information. This issue affects: Hitachi Energy LinkOne 3.20; 3.22; 3.23; 3.24; 3.25; 3.26.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-24265 Cuppa CMS v1.0 was discovered to contain a SQL injection vulnerability in /administrator/components/menu/ via the path=component/menu/&menu_filter=3 parameter.

HIGH Vector: network Created: 2022-01-31 Updated: 2022-02-03

CVE-2022-24266 Cuppa CMS v1.0 was discovered to contain a SQL injection vulnerability in /administrator/components/table_manager/ via the order_by parameter.

HIGH Vector: network Created: 2022-01-31 Updated: 2022-02-03

CVE-2022-24264 Cuppa CMS v1.0 was discovered to contain a SQL injection vulnerability in /administrator/components/table_manager/ via the search_word parameter.

HIGH Vector: network Created: 2022-01-31 Updated: 2022-02-03

CVE-2021-27654 Forgotten password reset functionality for local accounts can be used to bypass local authentication checks.

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-0392 Heap-based Buffer Overflow in **GitHub** repository vim/vim prior to 8.2.

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40340 Information Exposure vulnerability in **Hitachi** Energy LinkOne application, due to a misconfiguration in the ASP server exposes server and **ASP.net** information, an attacker that manages to exploit this vulnerability can use the exposed information as a reconnaissance for further exploitation. This issue affects: Hitachi Energy LinkOne 3.20; 3.22; 3.23; 3.24; 3.25; 3.26.

HIGH Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-46114 **jpress** v 4.2.0 is vulnerable to RCE via io.jpress.module.product.ProductNotifyKit#doSendEmail. The admin panel provides a function through which attackers can edit the email templates and inject some malicious code.

HIGH Vector: network Created: 2022-01-26 Updated: 2022-02-03

CVE-2021-46666 **MariaDB** before 10.6.2 allows an application crash because of mishandling of a pushdown from a HAVING clause to a WHERE clause.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46667 **MariaDB** before 10.6.5 has a sql_lex.cc integer overflow, leading to an application crash.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46663 **MariaDB** through 10.5.13 allows a ha_maria::extra application crash via certain SELECT statements.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46662 **MariaDB** through 10.5.9 allows a set_var.cc application crash via certain uses of an UPDATE statement in conjunction with a nested subquery.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46665 **MariaDB** through 10.5.9 allows a sql_parse.cc application crash because of incorrect used_tables expectations.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46661 **MariaDB** through 10.5.9 allows an application crash in find_field_in_tables and find_order_in_list via an unused common table expression (CTE).

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46664 **MariaDB** through 10.5.9 allows an application crash in sub_select_postjoin_aggr for a NULL value of aggr.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46668 **MariaDB** through 10.5.9 allows an application crash via certain long SELECT DISTINCT statements that improperly **interact** with storage-engine resource limitations for temporary data structures.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2021-46669 **MariaDB** through 10.5.9 allows attackers to trigger a convert_const_to_int use-after-free when the BIGINT data type is used.

HIGH Vector: network Created: 2022-02-01 Updated: 2022-02-03

CVE-2022-0393 Out-of-bounds Read in **GitHub** repository vim/vim prior to 8.2.

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-23727 There is a privilege escalation vulnerability in some webOS TVs. Due to wrong setting environments, local attacker is able to perform specific operation to exploit this vulnerability. Exploitation may cause the attacker to obtain a higher privilege

HIGH Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-23968 **Xerox** VersaLink devices on specific versions of firmware before 2022-01-26 allow remote attackers to brick the device via a crafted TIFF file in an unauthenticated HTTP POST request. There is a permanent denial of service because image parsing causes a reboot, but image parsing is restarted as soon as the boot process finishes. However, this boot loop can be resolved by a field technician. The TIFF file must have an incomplete Image Directory. Affected firmware versions include xx.42.01 and xx.50.61. NOTE: the 2022-01-24 NeoSmart article included "believed to affect all previous and later versions as of the **date** of this posting" but a 2022-01-26 vendor statement **reports** "the latest versions of firmware are not vulnerable to this issue."

HIGH Vector: network Created: 2022-01-26 Updated: 2022-02-03

Source: NIST

NIST CVE: Medium

CVE-2021-22819
A CWE-1021 Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause unintended modifications of the product settings or user accounts when deceiving the user to use the **web interface** rendered within iframes. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-22822
A CWE-79 Improper Neutralization of Input During Web Page Generation (?Cross-site Scripting?) vulnerability exists that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server. Affected Products: EVlink City EVC1S22P4 / EVC1S7P4 (All versions prior to R8 V3.4.0.2), EVlink Parking EVW2 / EVF2 / EVP2PE (All versions prior to R8 V3.4.0.2), and EVlink Smart Wallbox EVB1A (All versions prior to R8 V3.4.0.2)
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44390
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. Format param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44389
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. GetAbility param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44391
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. GetEnc param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44392
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. GetImage param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44393
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. GetIsp param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44395
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. GetMask param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44400
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. GetPtzPatrol param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44399
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. GetPtzPreset param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44402
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. GetPtzSerial param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44403
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. GetPtzTattern param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44404
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. GetZoomFocus param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44388
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. Login param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44396
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. Preview param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44401
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. PtzCtrl param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44397
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. rtmp=start param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44398
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. rtmp=stop param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44361
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. Set3G param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44383
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. SetAutoUpgrade param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44362
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. SetCloudSchedule param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44359
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. SetCrop param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44365
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. SetDevName param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44360
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. SetNorm param is not object. An attacker can send an HTTP request to trigger this vulnerability.
MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44386 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. SetPtzPatrol param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44387 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. SetPtzPreset param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44385 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. SetPtzSerial param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44363 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. SetPush param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44358 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. SetRec param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44364 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. SetWifi param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-44382 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.SetIrLights param is not object. An attacker can send an HTTP request to trigger this vulnerability.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40415 An incorrect default permission vulnerability exists in the cgiserver.cgi cgi_check_ability functionality of **reolink RLC-410W** v3.0.0.136_20121102. In cgi_check_ability the Format API does not have a specific case, the user permission will default to 7. This will give non-administrative users the possibility to format the SD card and reboot the device.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-22932 **Apache Karaf** obr:* commands and run goal on the karaf-maven-plugin have partial path traversal which allows to break out of expected folder. The risk is low as obr:* commands are not very used and the entry is set by user. This has been fixed in revision: https://gitbox.apache.org/repos/asf?p=karaf.git;h=36a2bc4 https://gitbox.apache.org/repos/asf?p=karaf.git;h=52b70cf Mitigation: Apache Karaf users should upgrade to 4.2.15 or 4.3.6 or later as soon as possible, or use correct path. **JIRA** Tickets: https://issues.apache.org/jira/browse/KARAF-7326

MEDIUM Vector: network Created: 2022-01-26 Updated: 2022-02-03

CVE-2021-31567 Authenticated (admin+) Arbitrary File Download vulnerability discovered in **Download Monitor WordPress** plugin (versions <= 4.4.6). The plugin allows arbitrary files, including sensitive configuration files such as wp-config.php, to be downloaded via the &downloadable_file_urls[0] parameter data. It's also possible to escape from the web server home directory and download any file within the OS.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-40338 **Hitachi** Energy LinkOne product, has a vulnerability due to a web server misconfiguration, that enables debug mode and reveals the full path of the filesystem directory when an attacker generates errors during a query operation. This issue affects: Hitachi Energy LinkOne 3.20; 3.22; 3.23; 3.24; 3.25; 3.26.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-23456 Potential arbitrary file deletion vulnerability has been identified in HP Support **Assistant** software.

MEDIUM Vector: local Created: 2022-01-28 Updated: 2022-02-03

CVE-2022-23889 The comment function in **YzmCMS** v6.3 was discovered as being able to be operated concurrently, allowing attackers to create an unusually large number of comments.

MEDIUM Vector: network Created: 2022-01-28 Updated: 2022-02-03

CVE-2021-46510 There is an Assertion `s < mjs->owned_strings.buf + mjs->owned_strings.len' failed at src/mjs_gc.c in **Cesanta** MJS v2.20.0.

MEDIUM Vector: local Created: 2022-01-27 Updated: 2022-02-03

CVE-2021-46506 There is an Assertion 'v->d.lval != v' failed at src/jsiValue.c in **Jsish** v3.5.0.

MEDIUM Vector: local Created: 2022-01-27 Updated: 2022-02-03

Source: NIST

NIST CVE: Low

CVE-2021-22799 A CWE-331: Insufficient Entropy vulnerability exists that could cause unintended connection from an internal network to an external network when an attacker manages to decrypt the SESU proxy password from the **registry**. Affected Product: Schneider Electric Software Update, V2.3.0 through V2.5.1

LOW Vector: local Created: 2022-01-28 Updated: 2022-02-03

Source: NIST

NIST CVE: Unrated

CVE-2021-45268 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.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-33627 A vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer(CommBuffer). This can be used by an attacker to corrupt data in SMRAM memory and even lead to arbitrary code execution.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-41840 A vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated table variable EFI_BOOT_SERVICES. This allows an attacker who is capable of executing code in DXE phase to exploit this vulnerability to escalate privileges to SMM. The attacker can overwrite the LocateProtocol or Freepool memory address location to execute unwanted code.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-41839 A vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated table variable EFI_BOOT_SERVICES. This can be used by an attacker to overwrite address location of any of the functions (FreePool,LocateHandleBuffer,HandleProtocol) to the address location of arbitrary code controlled by the attacker. On system call to SWSMI handler, the arbitrary code can be triggered to execute.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-41841 A vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated table variables EFI_BOOT_SERVICES and EFI_RUNTIME_SERVICES. This can be used by an attacker to overwrite address location of the function (LocateHandleBuffer) to the address location of arbitrary code controlled by the attacker. On system call to SWSMI handler, the arbitrary code can be triggered to execute.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-24069 An issue was discovered in AhciBusDxe in **Insyde** InsydeH2O with kernel 5.0 before 05.08.41, 5.1 before 05.16.29, 5.2 before 05.26.29, 5.3 before 05.35.29, 5.4 before 05.43.29, and 5.5 before 05.51.29. An SMM callout vulnerability allows an attacker to hijack the execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-33625 An issue was discovered in Kernel 5.x (starting from 5.1) in **Insyde** InsydeH2O, has a SMM memory corruption vulnerability allowing a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-24031 An issue was discovered in NvmExpressDxe in **Insyde** InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-43323 An issue was discovered in UsbCoreDxe in **Insyde** InsydeH2O with kernel 5.5 before 05.51.45, 5.4 before 05.43.45, 5.3 before 05.35.45, 5.2 before 05.26.45, 5.1 before 05.16.45, and 5.0 before 05.08.45. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-41838 An unsafe pointer vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler. An attacker can use this unsafe pointer "ptr" to read or write or manipulate data in the SMRAM. Exploitation of this vulnerability can lead to escalation of privileges reserved only for SMM using the SwSMI handler.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-39021 **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.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2022-24307 **Mastodon** before 3.3.2 and 3.4.x before 3.4.6 has incorrect access control because it does not compact incoming signed JSON-LD activities. (JSON-LD signing has been supported since version 1.6.0.)

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-23871 Multiple cross-site scripting (XSS) vulnerabilities in the component outcomes_addProcess.php of Gibbon CMS v22.0.01 allow attackers to execute arbitrary web scripts or HTML via a crafted payload insterted into the name, category, description parameters.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-42641 **PrinterLogic** Web Stack versions 19.1.1.13 SP9 and below are vulnerable to an Insecure Direct Object Reference (IDOR) vulnerability that allows an unauthenticated attacker to disclose the username and email address of all users.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2021-42639 **PrinterLogic** Web Stack versions 19.1.1.13 SP9 and below are vulnerable to multiple reflected cross site scripting vulnerabilities. Attacker controlled input is reflected back in the page without sanitization.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2021-42637 **PrinterLogic** Web Stack versions 19.1.1.13 SP9 and below use user-controlled input to craft a URL, resulting in a Server Side Request Forgery (SSRF) vulnerability.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2021-43615 SMM callout vulnerability allowing a possible attacker to hijack execution flow of a code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-42113 SMM callout vulnerability allowing a possible attacker to hijack execution flow of a code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-42554 SMM memory corruption vulnerability allowing a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could

CVE-2020-5953 A vulnerability exists in System Management Interrupt (SWSMI) handler of InsydeH2O UEFI Firmware code located in SWSMI handler that dereferences gRT (EFI_RUNTIME_SERVICES) pointer to call a GetVariable service, which is located outside of SMRAM. This can result in code execution in SMM (escalating privilege from ring 0 to ring -2).

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-43522 An issue was discovered in **Insyde** InsydeH2O with kernel 5.1 through 2021-11-08, 5.2 through 2021-11-08, and 5.3 through 2021-11-08. A StorageSecurityCommandDxe SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-23833 An issue was discovered in MultiPartParser in **Django** 2.2 before 2.2.27, 3.2 before 3.2.12, and 4.0 before 4.0.2. Passing certain inputs to multipart **forms** could result in an infinite loop when parsing files.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-44866 An issue was discovered in Online-Movie-Ticket-Booking-System 1.0. The file about.php does not perform input validation on the 'id' paramter. An attacker can append SQL queries to the input to extract sensitive information from the database.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-41837 An unsafe pointer vulnerability exists in SMM (System Management Mode) branch that registers a SWSMI handler. An attacker can use this unsafe pointer "current_ptr" to read or write or manipulate data into SMRAM. Exploitation of this vulnerability can lead to escalation of privileges reserved only for SMM using the SwSMI handler.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-22510 **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.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2022-22509 In **Phoenix** Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2022-23357 mozilo2.0 was discovered to be vulnerable to directory traversal attacks via the parameter curent_dir.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-42642 **PrinterLogic** Web Stack versions 19.1.1.13 SP9 and below are vulnerable to an Insecure Direct Object Reference (IDOR) vulnerability that allows an unauthenticated attacker to disclose the plaintext console username and password for a printer.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2021-42640 **PrinterLogic** Web Stack versions 19.1.1.13 SP9 and below are vulnerable to an Insecure Direct Object Reference (IDOR) vulnerability that allows an unauthenticated attacker to reassign drivers for any printer.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2021-42633 **PrinterLogic** Web Stack versions 19.1.1.13 SP9 and below are vulnerable to SQL Injection, which may allow an attacker to access additional audit records.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2022-0432 Prototype Pollution in **GitHub** repository mastodon/mastodon prior to 3.5.0.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2021-42060 SMM callout vulnerability allowing a possible attacker to hijack execution flow of a code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-24030 SMM memory corruption vulnerability allowing a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-24121 SQL Injection vulnerability discovered in Unified **Office** Total **Connect** Now that would allow an attacker to extract sensitive information

lead to escalating privileges to SMM.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2021-42059

Stack overflow vulnerability that allows a local root user to access UEFI DXE driver and execute arbitrary code.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-23569

Tensorflow is an Open Source Machine Learning **Framework**. Multiple operations in TensorFlow can be used to trigger a denial of service via `CHECK`-fails (i.e., assertion failures). This is similar to TFSA-2021-198 and has similar fixes. We have patched the reported issues in multiple **GitHub** commits. It is possible that other similar instances **exist** in TensorFlow, we will issue fixes as these are discovered. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21737

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `*Bincount` operations allows malicious users to cause denial of service by passing in arguments which would trigger a `CHECK`-fail. There are several conditions that the input arguments must satisfy. Some are not caught during **shape** inference and others are not caught during kernel implementation. This results in `CHECK` failures later when the output tensors get allocated. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21726

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `Dequantize` does not fully validate the value of `axis` and can result in heap OOB accesses. The `axis` argument can be `-1` (the default value for the optional argument) or any other positive value at most the number of **dimensions** of the input. Unfortunately, the upper bound is not checked and this results in reading past the end of the array containing the dimensions of the input tensor. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21735

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `FractionalMaxPool` can be made to crash a TensorFlow process via a division by 0. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21739

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `QuantizedMaxPool` has an undefined behavior where user controlled inputs can trigger a reference binding to 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21740

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `SparseCountSparseOutput` is vulnerable to a heap overflow. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21733

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `StringNGrams` can be used to trigger a denial of service attack by causing an out of memory condition after an integer overflow. We are missing a validation on `pad_witdh` and that result in computing a negative value for `ngram_width` which is later used to allocate parts of the output. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21729

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `UnravelIndex` is vulnerable to a division by zero caused by an integer overflow bug. 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.

through a **cookie** parameter.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-21741

Tensorflow is an Open Source Machine Learning **Framework**. ### Impact An attacker can craft a TFLite **model** that would trigger a division by zero in the implementation of depthwise convolutions. The parameters of the convolution can be user controlled and are also used within a division operation to **determine** the size of the padding that needs to be added before applying the convolution. There is no check before this division that the divisor is strictly positive. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21725

Tensorflow is an Open Source Machine Learning **Framework**. The estimator for the cost of some convolution operations can be made to execute a division by 0. The function fails to check that the stride argument is strictly positive. Hence, the fix is to add a check for the stride argument to ensure it is valid. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-23568

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `AddManySparseToTensorsMap` is vulnerable to an integer overflow which results in a `CHECK`-fail when building new `TensorShape` objects (so, an assert failure based denial of service). We are missing some validation on the shapes of the input tensors as well as directly constructing a large `TensorShape` with user-provided **dimensions**. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21730

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `FractionalAvgPoolGrad` does not consider cases where the input tensors are invalid allowing an attacker to read from outside of bounds of heap. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21734

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `MapStage` is vulnerable a `CHECK`-fail if the key tensor is not a scalar. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21738

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `SparseCountSparseOutput` can be made to crash a TensorFlow process by an integer overflow whose result is then used in a memory allocation. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21736

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `SparseTensorSliceDataset` has an undefined behavior: under certain condition it can be made to dereference a `nullptr` value. The 3 input arguments to `SparseTensorSliceDataset` represent a sparse tensor. However, there are some preconditions that these arguments must satisfy but these are not validated in the implementation. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21732

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of `ThreadPoolHandle` can be used to trigger a denial of service attack by allocating too much memory. This is because the `num_threads` argument is only checked to not be negative, but there is no upper bound on its value. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21731

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of **shape** inference for `ConcatV2` can be used to trigger a denial of service attack via a segfault caused by a type confusion. The `axis` argument is translated into `concat_dim` in the `ConcatShapeHelper` helper function. Then, a value for `min_rank` is computed based on `concat_dim`. This is then used to validate that the `values` tensor has at least the required rank. However, `WithRankAtLeast` receives the lower bound as a 64-bits value and then compares it against the maximum 32-bits integer value that could be represented. Due to the fact that `min_rank` is a 32-bits value and the value of `axis`, the `rank` argument is a negative value, so the error

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

check is bypassed. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21727

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of **shape** inference for `Dequantize` is vulnerable to an integer overflow weakness. The `axis` argument can be `-1` (the default value for the optional argument) or any other positive value at most the number of **dimensions** of the input. Unfortunately, the upper bound is not checked, and, since the code computes `axis + 1`, an attacker can trigger an integer overflow. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-21728

Tensorflow is an Open Source Machine Learning **Framework**. The implementation of **shape** inference for `ReverseSequence` does not fully validate the value of `batch_dim` and can result in a heap OOB read. There is a check to make sure the value of `batch_dim` does not go over the rank of the input, but there is no check for negative values. Negative **dimensions** are allowed in some cases to mimic Python's negative indexing (i.e., indexing from the end of the array), however if the value is too negative then the implementation of `Dim` would access elements before the start of an array. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-23567

Tensorflow is an Open Source Machine Learning **Framework**. The implementations of `Sparse*Cwise*` ops are vulnerable to integer overflows. These can be used to trigger large allocations (so, OOM based denial of service) or `CHECK`-fails when building new `TensorShape` objects (so, assert failures based denial of service). We are missing some validation on the shapes of the input tensors as well as directly constructing a large `TensorShape` with user-provided **dimensions**. 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: 2022-02-03 Updated: 2022-02-03

CVE-2022-22818

The {% debug %} template tag in **Django** 2.2 before 2.2.27, 3.2 before 3.2.12, and 4.0 before 4.0.2 does not properly encode the current context. This may lead to XSS.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

CVE-2022-0443

Use After Free in Conda vim prior to 8.2.

UNRATED Vector: unkown Created: 2022-02-02 Updated: 2022-02-03

CVE-2022-23873

Victor CMS v1.0 was discovered to contain a SQL injection vulnerability that allows attackers to inject arbitrary commands via 'user_firstname' parameter.

UNRATED Vector: unkown Created: 2022-02-03 Updated: 2022-02-03

Source: Hybrid Analysis

Top malicious files

100% Threat score	Amazon AIO (.) exe	100% Threat score	decoded-2 (.) exe
100% Threat score	RUWirelessSecure (.) exe	100% Threat score	Spotify (.) exe
100% Threat score	GM322018576172016 (.) xls	100% Threat score	Activate___Full__Setup----4695 (.) exe
100% Threat score	2022-02-03_1559 (.) xls	100% Threat score	megumi_final (.) dll
95% Threat score	ipscan-win32-3 (.) 5 (.) 1 (.) exe	85% Threat score	VCredist_arm64 (.) exe
85% Threat score	vcredist_x64 (.) exe	85% Threat score	vcredist_x86 (.) exe
85% Threat score	Click_Here_Now_to_Continue_to_WilfireVPN-v16 (.) msi	84% Threat score	Ghost64 (.) exe
73% Threat score	3389 (.) exe	71% Threat score	USB Show (.) exe

Source: Hybrid Analysis

Top malicious URL

100% Threat score	http://222 (.) 141 (.) 12 (.) 100:47290/Mozi (.) m	100% Threat score	http://27 (.) 6 (.) 91 (.) 98:53874/Mozi (.) a
100% Threat score	http://27 (.) 43 (.) 109 (.) 234:50730/Mozi (.) a	100% Threat score	http://27 (.) 215 (.) 210 (.) 164:36695/Mozi (.) m
94% Threat score	http://viewsultimate (.) getforge (.) io/	87% Threat score	https://app (.) getresponse (.) com/click (.) html?x=a62b&lc=SqRlwV&mc=rk&s=0ilJlC&u=BVvpd&z=E
81% Threat score	https://ronemo (.) com/video/HrJ3D2P9bzB/JbR4Ggv3Pz	78% Threat score	http://u6152414 (.) ct (.) sendgrid (.) net/
78% Threat score	http://globaloceanhealth (.) org/wp-content/plugins/social-media-widget/social_widget (.) css?ver=5 (.) 8 (.) 3	77% Threat score	https://nam10 (.) safelinks (.) protection (.) outlook (.) com/?url=http%3A%2F%2F6790 (.) 07 (.) idpro (.) co (.) id%2FvjR14Z6i0U%2FaHR0cHM6Ly9vYmplY3RzdG9yYWdlLnVzLWFzaGJ1cm4tMS5vcmFjbGVjbG91ZC5jb20vbi9pZHFpcWJubW com%7C437bf9fe46d54822fa1b08d9e759f592%7Cd5f1622b14a345a6b069003f8dc4851f%7C0%7C0%7C637795195839302997%

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 hosters

#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 Viet Nam
- #8 Brazil
- #9 Pakistan
- #10 Iran (Islamic Republic of)

Source: SpamHaus

Top phishing countries

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