Your Security Rabbits report for February 02, 2022

Hot topics

Nothing today

News

IT Security Guru

AI-powered tools to fend off ransomware attacks

Zero trust-type security has become the standard for any self-respecting security software provider and is a step in the right direction in the never-ending battle against the bad hacker actors of the worlds. Unfortunately, it doesn't seem the be the final answer to storing corporate data securely for an enterprise and its users. Zero trust [...] The post AI-powered tools to fend off ransomware attacks appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Arid Viper Hackers Strike Palestinian Targets with Political Lures and Trojans

In the past, the group has been responsible for spear phishing attacks against Palestinian law enforcement, the military, educational establishments, and the Israel Security Agency (ISA).

IT Security Guru

Cato Networks delivers first CASB for instant visibility and control of cloud application data risk

Cato Networks yesterday announced the release of Cato CASB, the first Cloud Access Security Broker (CASB) to help companies with visibility and managing cloud application data risk. This new offering "addresses a critical visibility and control gap created by cloud migration but must be converged into a broad SASE platform to be truly effective across [...] The post Cato Networks delivers first CASB for instant visibility and control of cloud application data risk appeared first on IT Security Guru.

IT Security Guru

Cloudflare launches paid public bug bounty program

The American web infrastructure and website security company Cloudflare has announced the launch of a new public bug bounty program. Rushil Shah, a Product Security Engineer at Cloudflare said, "today we are launching Cloudflare's paid public bug bounty program," "We believe bug bounties are a vital part of every security team's toolbox and have been [...] The post Cloudflare launches paid public bug bounty program appeared first on IT Security Guru.

The Hacker News

Critical Bug Found in WordPress Plugin for Elementor with Over a Million Installations

A WordPress plugin with over one million installs has been found to contain a critical vulnerability that could result in the execution of arbitrary code on compromised websites. The plugin in question is Essential Addons for Elementor, which provides WordPress site owners with a library of over 80 elements and extensions to help design and customize pages and posts. "This vulnerability allows

IT Security Guru

Data Leak Exposes IDs of Airport Security Workers

A cloud misconfiguration has leaked personal details of countless airport staff throughout South America, a new report suggests. An Amazon Web Services S3 bucket was found without any authentication required to access its contents. A team at AV comparison site Safety Detectives found the problem and notified the owner, Swedish security giant Securitas on October [...] The post Data Leak Exposes IDs of Airport Security Workers appeared first on IT Security Guru.

CyberScoop

DHS assembles Cyber Safety Review Board to imitate fed agency that studies aviation accidents

The Homeland Security Department is establishing a Cyber Safety Review Board that will convene after major cyber events to review and act on them, according to a Federal Register notice scheduled for publication Thursday. The Federal Register notice brings to fruition an idea long circulated among cybersecurity policymakers and thinkers, one set in motion by an executive order President Joe Biden signed in May 2021. The idea is to mimic the National Transportation Safety Board that reviews civil aviation accidents. The board (CSRB) will have no more than 20 members, with one each required from DHS, its Cybersecurity and Infrastructure Protection Agency, the Department of Justice, the Nationa[...]

ZDNet | security RSS

Arid Viper hackers strike Palestine with political lures and Trojans

The threat group is suspected of being located in Gaza.

IT Security Guru

Business leaders are confident in their defences, despite over half falling victim to ransomware

New research from Adarma, the UK's largest independent cyber threat management company, has discovered a major disconnect in the way organisations think and act in the face of ransomware. Adarma's nationwide ransomware study surveyed 500 C-level executives at UK businesses with over 2,000 employees and found that 58% of respondents have experienced a ransomware attack, with [...] The post Business leaders are confident in their defences, despite over half falling victim to ransomware appeared first on IT Security Guru.

Threatpost

Charming Kitten Sharpens Its Claws with PowerShell Backdoor

The notorious Iranian APT is fortifying its arsenal with new malicious tools and evasion tactics and may even be behind the Memento ransomware.

Cyware News - Latest Cyber News

CoinStomp Malware Targets Asian Cloud Service Providers to Mine Monero

Researchers say that the purpose of CoinStomp is to quietly compromise instances in order to harness computing power to illicit mine for cryptocurrency, a form of attack known as cryptojacking.

The Hacker News

Cynet's Keys to Extend Threat Visibility

We hear about the need for better visibility in the cybersecurity space - detecting threats earlier and more accurately. We often hear about the dwell time and the time to identify and contain a data breach. Many of us are familiar with IBM's Cost of a Data Breach Report that has been tracking this statistic for years. In the 2021 report, IBM found that, on average, it takes an average of 212

Cyware News - Latest Cyber News

DeadBolt Hits QNAP Hard, 3600 Devices Impacted

A new DeadBolt ransomware group encrypted more than 3,600 network-attached storage (NAS) devices worldwide by exploiting a zero-day with the most affected countries being the U.S., France, Taiwan, Italy, and the U.K. QNAP has warned customers to protect their devices by updating the QTS software version and disabling port forwarding and UPnP.

The Hacker News

Dozens of Security Flaws Discovered in UEFI Firmware Used by Several Vendors

As many as 23 new high severity security vulnerabilities have been disclosed in different implementations of Unified Extensible Firmware Interface (UEFI) firmware used by numerous vendors, including Bull Atos, Fujitsu, HP, Juniper Networks, Lenovo, among others. The vulnerabilities reside in Insyde Software's InsydeH2O UEFI firmware, according to enterprise firmware security company Binarly,

ESET Patches High-Severity Vulnerability in Windows Applications

Naked Security

Elementor WordPress plugin has a gaping security hole - update now
We shouldn't need to say, "Check your inputs!" these days, but we're saying it anyway.

Cyware News - Latest Cyber News

Tracked as CVE-2021-37852 and reported to ESET by the Zero Day Initiative (ZDI), the vulnerability is considered "high severity," as it could allow an attacker to misuse the AMSI scanning feature.

Security Affairs

ESET releases fixes for local privilege escalation bug in Windows Applications
Antivirus firm ESET addressed a local privilege escalation vulnerability, tracked CVE-2021-37852, impacting its Windows clients. Antivirus firm ESET released security patches to address a high severity local privilege escalation vulnerability, tracked CVE-2021-37852, impacting its Windows clients. An attacker can exploit the vulnerability to misuse the AMSI scanning feature to elevate privileges in specific scenarios. "According [...] The post ESET releases fixes for local privilege escalation bug in Windows Applications appeared first on Security Affairs.

Security Affairs

Experts found 23 flaws in UEFI firmware potentially impact millions of devices
Researchers discovered tens of vulnerabilities in UEFI firmware code used by the major device manufacturers. Researchers at firmware security company Binarly have discovered 23 vulnerabilities in UEFI firmware code used by the major device makers. The vulnerabilities could impact millions of enterprise devices, including laptops, servers, routers, and industrial control systems (ICS). All these vulnerabilities [...] The post Experts found 23 flaws in UEFI firmware potentially impact millions of devices appeared first on Security Affairs.

Security Affairs

Experts warn of a spike in APT35 activity and a possible link to Memento ransomware op
The Cybereason Nocturnus Team reported a spike in the activity of the Iran-linked APT group APT35 (aka Phosphorus or Charming Kitten). The Cybereason Nocturnus Team observed a spike in the activity of the Iran-linked APT group APT35 (aka 'Charming Kitten', 'Phosphorus', Newscaster, and Ajax Security Team) The Phosphorus group made the headlines in 2014 when experts at iSight issued a report describing the most elaborate net-based spying campaign organized [...] The post Experts warn of a spike in APT35 activity and a possible link to Memento ransomware op appeared first on Security Affairs.

Cyware News - Latest Cyber News

Fastly patches memory leak HTTP/3 vulnerability in H2O HTTP server project
An uninitialized memory leak vulnerability in the H2O HTTP server project has been patched. H20 is an open-source optimization project for HTTP/1, HTTP/2, and HTTP/3 servers

IT Security Guru

FBI warns of scam job listings
Scammers are conducting phishing campaigns using fake advertisements on recruitment platforms. The FBI issued the warning today through a public service announcement (PSA) on their Internet Crime Complaint Centre (IC3). "The FBI warns that malicious actors or 'scammers' continue to exploit security weaknesses on job recruitment websites to post fraudulent job postings in order to [...] The post FBI warns of scam job listings appeared first on IT Security Guru.

Threatpost

FBI: Use a Burner Phone at the Olympics
The warning follows a Citizen Lab report that found the official, mandatory app has an encryption flaw that "can be trivially sidestepped." Besides burners, here are more tips on staying cyber-safe at the Games.

Blog â€" Flashpoint

Following a Transformative Year, Flashpoint Kicks Off 2022 Announcing Record Growth, Key Product Innovations, National Security Business Expansion, and a New Acquisition
NEW YORK, NY - February 2, 2022 -- Flashpoint, the trusted leader in threat intelligence and risk prevention, is celebrating record momentum following the close of calendar year 2021. By providing organizations with the threat intelligence and automation they require to rapidly detect, prioritize, and combat cyber, fraud, and physical risks during a tumultuous year, [...] The post Following a Transformative Year, Flashpoint Kicks Off 2022 Announcing Record Growth, Key Product Innovations, National Security Business Expansion, and a New Acquisition appeared first on Flashpoint.

Cyware News - Latest Cyber News

Google Patches 27 Vulnerabilities With Release of Chrome 98
Of the 19 flaws, 8 carry a severity rating of high, 10 are medium severity, and one is low risk. Over half of the externally reported vulnerabilities addressed in this release are use-after-free bugs.

The Hacker News

Hacker Group 'Moses Staff' Using New StrifeWater RAT in Ransomware Attacks
A politically motivated hacker group tied to a series of espionage and sabotage attacks on Israeli entities in 2021 incorporated a previously undocumented remote access trojan (RAT) that masquerades as the Windows Calculator app as part of a conscious effort to stay under the radar. Cybersecurity company Cybereason, which has been tracking the operations of the Iranian actor known as Moses Staff

Cyware News - Latest Cyber News

Is REvil Active Even After Arrests?
Even after the recent arrest of the members of the REvil ransomware group, researchers have found multiple samples being deployed across targets. After the arrests, the number of REvil implants dipped to 24 per day, but that again increased to 26 implants a day. Today, it is highly obscure whether these raids and arrests of high-profile arrests of affiliates are actually making a difference.

Threatpost

KP Snacks Left with Crumbs After Ransomware Attack
The Conti gang strikes again, disrupting the nom-merchant's supply chain and threatening empty supermarket shelves lasting for weeks.

Cyware News - Latest Cyber News

Lazarus Pushes Malware by Placing Job Offers
Lazarus APT group, infamous for targeting the defense industry, now abuses Windows Update Client to spread malware. It was recently observed masquerading as Lockheed Martin in spear-phishing campaigns. For the first time in this campaign, the group had used GitHub as a C2 for targeted and short-term attacks. Take the right measure to safeguard your national security systems.

Cyware News - Latest Cyber News

Malware Used by SolarWinds Hack Culprit Nobelium Group Went Undetected for Years
Two sophisticated malware families were placed on victim systems -- a Linux variant of GoldMax and a new implant dubbed TrailBlazer -- long before the scale of the attacks came to light.

Cyware News - Latest Cyber News

Massive Social Engineering Campaigns Impacted Banks in Europe and South America
The campaigns, which aim to steal banking secrets and payment cards of users, are carried out by using social engineering schemas, namely smishing, and spear-phishing through fake emails.

Security Affairs

Massive social engineering waves have impacted banks in several countries
A massive social engineering campaign targeting banks has been delivered in the last two years in several countries. A massive social engineering campaign has been delivered in the last two years in several countries, including Portugal, Spain, Brazil, Mexico, Chile, the UK, and France. According to Seguranca Informatica publication, the malicious waves have impacted banking [...] The post Massive social engineering waves have impacted banks in several countries appeared first on Security Affairs.

ZDNet | security RSS

Meet CoinStomp: New cryptojacking malware targets Asian cloud service providers
Shell scripts are being used to exploit cloud instances.

The Hacker News

New Malware Used by SolarWinds Attackers Went Undetected for Years
The threat actor behind the supply chain compromise of SolarWinds has continued to expand its malware arsenal with new tools and techniques that were deployed in attacks as early as 2019, once indicative of the elusive nature of the campaigns and the adversary's ability to maintain persistent access for years. According to cybersecurity firm CrowdStrike, which detailed the novel tactics adopted

Security Affairs

Researcher found an Information Disclosure in the Brave browser
Security researcher discovered an Information Disclosure vulnerability in Brave browser and reported it through the HackerOne platform. Security researcher Kirtikumar Anandrao Ramchandani discovered an Information Disclosure vulnerability in the Brave Browser and reported it to the company through the HackerOne platform. The researcher discovered that when the browser is used with Tor it could leak [...] The post Researcher found an Information Disclosure in the Brave browser appeared first on Security Affairs.

CyberScoop

Researchers detect fresh wave of hacking attacks on Palestinian targets

A hacking group is targeting Palestinian people and organizations with a wave of years-old malware, according to research published Wednesday. The findings, from Cisco's Talos threat intelligence division, unpack a surge of attacks starting around October 2021 targeting Palestinians using malware known as Micropsia. The attacks are part of a broader campaign dating back to 2017 connected to a group known as Arid Viper, an Arabic hacking group possibly associated with Hamas that first emerged in 2015. Also known as Desert Falcons or APT-C-23, -- "APT" stands for "advanced persistent threat," a kind of group often associated with nation-state hackers --Kaspersky researchers in 2015 named it th[...]

IT Security Guru

Salt Security brings API security to the channel

Salt Security, the API security company, has announced the global expansion of its Salt Security Essential Partner Program, with the company noting that it will be instrumental in ensuring customers around the world can protect the APIs fueling their digital transformations, application modernisations, cloud migrations, and other digital initiatives. The company state that it has [...] The post Salt Security brings API security to the channel appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Scottish Agency Still Recovering from 2020 Ransomware Attack

Despite claiming the agency had a "high" level of cyber-maturity, independent reviews since the attack have also made 44 recommendations for enhancing the agency's cyber-readiness and resilience.

WeLiveSecurity

Shoulder surfing: Watch out for eagle-eyed snoopers peeking at your phone

Some fraudsters may use low-tech tactics to steal your sensitive information - peering over your shoulder as you enter that data is one of them The post Shoulder surfing: Watch out for eagle-eyed snoopers peeking at your phone appeared first on WeLiveSecurity

CyberScoop

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

The State Department is offering a $10 million reward for information on two Iranian hackers who allegedly participated in state-sponsored cyber operations designed to interfere with the 2020 U.S. presidential election. The two individuals, Seyyed Mohammad Hosein Musa Kazemi, 24, and Sajjad Kashian, 27, were charged with computer fraud, voter intimidation and transmission of interstate threats according to a federal indictment unsealed in November. The activity took place between August 2020 and November 2020. The State Department is offering the reward under its "Rewards for Justice" program, which has posted equal bounties for information about ransomware groups DarkSide and REvil. The ind[...]

Security Affairs

Sugar Ransomware, a new RaaS in the threat landscape

Cyber security team at retail giant Walmart dissected a new ransomware family dubbed Sugar, which implements a ransomware-as-a-service model. The cyber threat team at retail giant Walmart has analyzed a new ransomware family dubbed Sugar, which is offered through a ransomware-as-a-service (RaaS) model. Unlike other ransomware operations, Sugar ransomware appears to primarily focus on individual [...] The post Sugar Ransomware, a new RaaS in the threat landscape appeared first on Security Affairs.

Threatpost

Supply-Chain Security Is Not a Problem...It's a Predicament

Despite what security vendors might say, there is no way to comprehensively solve our supply-chain security challenges, posits JupiterOne CISO Sounil Yu. We can only manage them.

Cyware News - Latest Cyber News

Tenable agrees to acquire Cymptom; terms undisclosed (NASDAQ:TENB)

Tenable has agreed to acquire Cymptom, a specialist in attack path management. The financial terms of the deal were not disclosed. The acquisition is expected to close in Q122.

Threatpost

Thousands of Malicious npm Packages Threaten Web Apps

Attackers increasingly are using malicious JavaScript packages to steal data, engage in cryptojacking and unleash botnets, offering a wide supply-chain attack surface for threat actors.

Twitter

CyCatz

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

Ptrace Security GmbH

PoC for CVE-2021-45897 #Pentesting #CyberSecurity #Infosec

Cyber Advising

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

blueblue

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

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2022-23967 Description: In TightVNC 1.3.10, there is an integer signedness error and resultant heap-base... CVSS: 9.52 #tightvnc #tightvnc #CVE #CyberSecurity #DataBreach

Nicholas Carroll

You know someone is in for a bad weekend when a #POC hits GitHub and there's vulnerable systems indexed in Shodan. Check out the code for CVE-2022-23967 by Maher Azzouzi for all your TightVNC buffer overflow needs at

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2022-0362 Description: SQL Injection in Packagist showdoc/showdoc prior to 2.10.3.... CVSS: 9.12 #showdoc #showdoc #CVE #CyberSecurity #DataBreach

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2021-45435 Description: An SQL Injection vulnerability exists in Sourcecodester Simple Cold Storage Mana... CVSS: 9.44 #sourcecodester #complaint_management #CVE #CyberSecurity #DataBreach

Prophaze Web Security Platform

ShowDoc up to 2.10.2 sql injection [CVE-2022-0362] #Exploit:No #Local:No #Product:ShowDoc #Remote:Yes

CVE

CVE-2021-44249 Online Motorcycle (Bike) Rental System 1.0 is vulnerable to a Blind Time-Based SQL Injection attack within the login portal. This can lead attackers to remotely dump MySQL database credentials.

Prophaze Web Security Platform

mingsoft MCMS up to 5.2.5 unrestricted upload [CVE-2021-46386] #Exploit:Yes #Local:No #Product:MCMS #Remote:Yes

Robo Shadow Alerts

Potentially Critical CVE Detected! CVE-2021-41609 Description: SQL injection in the ID parameter of the UploadedImageDisplay.aspx endpoint of S... CVSS: 9.58 #classapps #selectsurvey.net #CVE #CyberSecurity #DataBreach

Source: NIST

NIST CVE: Critical

CVE-2021-46428

A Remote Code Execution (RCE) vulnerability exists in **Sourcecodester** Simple Chatbot Application 1.0 (and previous versions via the bot_avatar parameter in SystemSettings.php.

CVE-2022-22294

A SQL injection vulnerability exists in ZFAKA<=1.43 which an attacker can use to complete SQL injection in the foreground and add a background administrator account.

CRITICAL | Vector: network | Created: 2022-01-27 | Updated: 2022-02-02

CVE-2022-23097

An issue was discovered in the DNS proxy in **Connman** through 1.40. forward_dns_reply mishandles a strnlen call, leading to an out-of-bounds read.

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

CVE-2021-46427

An SQL Injection vulnerability exists in **Sourcecodester** Simple Chatbot Application 1.0 via the message parameter in Master.php.

CRITICAL | Vector: network | Created: 2022-01-27 | Updated: 2022-02-02

CVE-2020-25905

An SQL Injection vulnerabilty exists in **Sourcecodester** Mobile Shop System in PHP **MySQL** 1.0 via the email parameter in (1) login.php or (2) LoginAsAdmin.php.

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

CVE-2022-24219

eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_page.php.

CRITICAL | Vector: network | Created: 2022-02-01 | Updated: 2022-02-02

CVE-2022-24222

eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_user.php.

CRITICAL | Vector: network | Created: 2022-02-01 | Updated: 2022-02-02

CVE-2021-46446

H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/admin.php?module=admin_access_group_edit&aagID.

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

CVE-2021-46445

H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/categories.php?box_group_id.

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

CVE-2022-0392

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

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

CVE-2022-23967

In **TightVNC** 1.3.10, there is an integer signedness error and resultant heap-based buffer overflow in InitialiseRFBConnection in rfbproto.c (for the **vncviewer** component). There is no check on the size given to malloc, e.g., -1 is accepted. This allocates a chunk of size zero, which will give a heap pointer. However, one can send 0xffffffff bytes of data, which can have a DoS impact or lead to remote code execution.

CRITICAL | Vector: network | Created: 2022-01-26 | Updated: 2022-02-02

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: 2022-02-02

CVE-2022-0393

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

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

CVE-2022-21723

PJSIP is a free and open source multimedia communication

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

CVE-2022-23096

An issue was discovered in the DNS proxy in **Connman** through 1.40. The TCP server reply implementation lacks a check for the presence of sufficient Header Data, leading to an out-of-bounds read.

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

CVE-2021-45435

An SQL Injection vulnerability exists in **Sourcecodester** Simple Cold Storage Management System using PHP/OOP 1.0 via the username field in login.php.

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

CVE-2021-46093

eliteCMS v1.0 is vulnerable to Insecure Permissions via manage_uploads.php.

CRITICAL | Vector: network | Created: 2022-02-01 | Updated: 2022-02-02

CVE-2022-24220

eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/edit_post.php.

CRITICAL | Vector: network | Created: 2022-02-01 | Updated: 2022-02-02

CVE-2022-24221

eliteCMS v1.0 was discovered to contain a SQL injection vulnerability via /admin/functions/functions.php.

CRITICAL | Vector: network | Created: 2022-02-01 | Updated: 2022-02-02

CVE-2021-46444

H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/admin.php?module=admin_group_edit&agID.

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

CVE-2021-46448

H.H.G Multistore v5.1.0 and below was discovered to contain a SQL injection vulnerability via /admin/customers.php?page=1&cID.

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

CVE-2021-46386

https://gitee.com/mingSoft/MCMS MCMS <=5.2.5 is affected by: File Upload. The impact is: execute arbitrary code (remote). The component is: net.mingsoft.basic.action.web.FileAction#upload. The attack vector is: jspx webshell. PP MCMS has a file upload vulnerability through which attacker can upload a webshell. Successful attacks of this vulnerability can result in takeover of MCMS

CRITICAL | Vector: network | Created: 2022-01-26 | Updated: 2022-02-02

CVE-2021-44971

Multiple **Tenda** devices are affected by authentication bypass, such as AC15V1.0 Firmware V15.03.05.20_multi?AC5V1.0 Firmware V15.03.06.48_multi and so on. an attacker can obtain sensitive information, and even combine it with authenticated command injection to implement RCE.

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

CVE-2021-44249

Online Motorcycle (Bike) Rental System 1.0 is vulnerable to a Blind Time-Based SQL Injection attack within the login **portal**. This can lead attackers to remotely dump **MySQL** database credentials.

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

CVE-2022-21722

PJSIP is a free and open source multimedia communication library written in C language implementing **standard** based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In version 2.11.1 and prior, there are various cases where it is possible that certain incoming RTP/RTCP packets can potentially cause out-of-bound read access. This issue affects all users that use PJMEDIA and accept incoming RTP/RTCP. A patch is available as a commit in the `master` branch. There are no known workarounds.

CRITICAL | Vector: network | Created: 2022-01-27 | Updated: 2022-02-02

library written in C language implementing **standard** based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In versions 2.11.1 and prior, parsing an incoming SIP message that contains a malformed multipart can potentially cause out-of-bound read access. This issue affects all PJSIP users that accept SIP multipart. The patch is available as commit in the `master` branch. There are no known workarounds.

CRITICAL Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2022-0362

SQL Injection in Packagist showdoc/showdoc prior to 2.10.3.

CRITICAL Vector: network Created: 2022-01-26 Updated: 2022-02-02

CVE-2021-41609

SQL injection in the ID parameter of the UploadedImageDisplay.aspx **endpoint** of SelectSurvey.NET before 5.052.000 allows a remote, unauthenticated attacker to retrieve data from the application's backend database via boolean-based blind and UNION injection.

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

CVE-2021-45898

SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows local file inclusion.

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

CVE-2021-45899

SuiteCRM before 7.12.3 and 8.x before 8.0.2 allows PHAR deserialization that can lead to remote code execution.

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

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: 2022-02-02

CVE-2021-43799

Zulip is an open-source team **collaboration** tool. **Zulip Server** installs **RabbitMQ** for internal message passing. In versions of Zulip Server prior to 4.9, the initial installation (until **first** reboot, or restart of RabbitMQ) does not successfully limit the default ports which RabbitMQ opens; this includes port 25672, the RabbitMQ distribution port, which is used as a management port. RabbitMQ's default "cookie" which protects this port is generated using a weak PRNG, which limits the entropy of the password to at most 36 bits; in practicality, the seed for the randomizer is biased, resulting in approximately 20 bits of entropy. If other firewalls (at the OS or network level) do not protect port 25672, a remote attacker can brute-force the 20 bits of entropy in the "cookie" and leverage it for arbitrary execution of code as the rabbitmq user. They can also read all data which is sent through RabbitMQ, which includes all message traffic sent by users. Version 4.9 contains a patch for this vulnerability. As a workaround, ensure that firewalls prevent access to ports 5672 and 25672 from outside the Zulip server.

CRITICAL Vector: network Created: 2022-01-25 Updated: 2022-02-02

CVE-2021-46377

There is a front-end sql injection vulnerability in **cszcms** 1.2.9 via cszcms/controllers/Member.php#viewUser

CRITICAL Vector: network Created: 2022-01-27 Updated: 2022-02-02

Source: NIST

NIST CVE: High

CVE-2021-22724

A CVE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could allow an attacker to impersonate the user or carry out actions on their behalf when crafted malicious parameters are submitted in POST requests sent 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: 2022-02-02

CVE-2021-22725

A CVE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could allow an attacker to impersonate the user or carry out actions on their behalf when crafted malicious parameters are submitted in POST requests sent 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: 2022-02-02

CVE-2021-22808

A CWE-416: Use After Free vulnerability exists that could cause arbitrary code execution when a malicious *.gd1 configuration file is loaded into the **GUIcon** tool. Affected Product: Eurotherm by Schneider Electric GUIcon Version 2.0 (Build 683.003) and prior

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

CVE-2021-22807

A CWE-787: Out-of-bounds Write vulnerability exists that could cause arbitrary code execution when a malicious *.gd1 configuration file is loaded into the **GUIcon** tool. Affected Product: Eurotherm by Schneider Electric GUIcon Version 2.0 (Build 683.003) and prior

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

CVE-2021-41608

A file disclosure vulnerability in the UploadedImageDisplay.aspx **endpoint** of SelectSurvey.NET before 5.052.000 allows a remote, unauthenticated attacker to retrieve survey user submitted data by modifying the value of the ID parameter in sequential order beginning from 1.

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

CVE-2022-22828

An insecure direct object reference for the file-download URL in **Synametrics SynaMan** before 5.0 allows a remote attacker to access unshared files via a modified base64-encoded filename string.

HIGH Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2022-23098

An issue was discovered in the DNS proxy in **Connman** through 1.40. The TCP server reply implementation has an infinite loop if no data is received.

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

CVE-2021-42791

An issue was discovered in VeridiumID VeridiumAD 2.5.3.0. The **HTTP request** to trigger **push notifications** for VeridiumAD enrolled users does not enforce proper access control. A user can trigger push notifications for any other user. The text contained in the push notification can also be modified. If a user who receives the notification accepts it, then the user who triggered the notification can obtain the accepting user's login certificate.

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

CVE-2021-46097

Dolphinphp v1.5.0 contains a remote code execution vulnerability in /application/common.php#action_log

HIGH Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2021-32849

Gerapy is a distributed crawler management **framework**. Prior to version 0.9.9, an authenticated user could execute arbitrary commands. This issue is fixed in version 0.9.9. There are no known workarounds.

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

CVE-2022-0361

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

CVE-2022-0359

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

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

CVE-2021-46383

https://gitee.com/mingSoft/MCMS MCMS <=5.2.5 is affected by: SQL Injection. The impact is: obtain sensitive information (remote). The component is: net.mingsoft.mdiy.action.web.DictAction#list. The attack vector is: 0 or sleep(3). PP MCMS has a sql injection vulnerability through which attacker can get sensitive information from the database.

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

CVE-2021-45975

In ListCheck.exe in **Acer** Care Center 4.x before 4.00.3038, a vulnerability in the loading mechanism of **Windows** DLLs could allow a local attacker to perform a DLL hijacking attack. This vulnerability is due to incorrect handling of directory search paths at run time. An attacker could exploit this vulnerability by placing a malicious DLL file on the targeted system. This file will execute when the vulnerable application launches. A successful exploit could allow the attacker to execute arbitrary code on the targeted system with local administrator privileges.

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

CVE-2021-46116

jpress 4.2.0 is vulnerable to remote code execution via io.jpress.web.admin._TemplateController#doInstall. The admin panel provides a function through which attackers can install templates and inject some malicious code.

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

CVE-2020-28884

Liferay Portal Server tested **on 7**.3.5 GA6, 7.2.0 GA1 is affected by OS Command Injection. An administrator user can inject **Groovy** script to execute any OS command on the **Liferay Portal** Sever.

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

CVE-2022-23013

On **BIG-IP** DNS & GTM version 16.x before 16.1.0, 15.1.x before 15.1.4, 14.1.x before 14.1.4.4, and all versions of 13.1.x, 12.1.x, and 11.6.x, a DOM-based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the **BIG-IP Configuration utility** that allows an attacker to execute JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

HIGH Vector: network Created: 2022-01-25 Updated: 2022-02-02

CVE-2016-3735

Piwigo is image **gallery** software written in PHP. When a criteria is not met on a host, piwigo defaults to usingmt_rand in order to generate password reset tokens. mt_rand output can be predicted after recovering the seed used to generate it. This low an unauthenticated attacker to take over an account providing they know an administrators email address in order to be able to request password reset.

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

CVE-2021-42638

PrinterLogic Web Stack versions 19.1.1.13 SP9 and below do not sanitize user input resulting in pre-auth remote code execution.

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

CVE-2021-44795

Single **Connect** does not perform an authorization check when using the "sc-assigned-credential-ui" module. A remote attacker could exploit this vulnerability to modify users permissions. The exploitation of this vulnerability might allow a remote attacker to delete permissions from other users without authenticating.

HIGH Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2021-44122

SPIP 4.0.0 is affected by a Cross Site Request Forgery (CSRF) vulnerability in ecrire/public/aiguiller.php, ecrire/public/balises.php, ecrire/balise/formulaire_.php. To exploit the vulnerability, a visitor must visit a malicious website which redirects to the SPIP website. It is also possible to combine XSS vulnerabilities in SPIP 4.0.0 to exploit it. The vulnerability allows an authenticated attacker to execute malicious code without the knowledge of the user on the website (CSRF).

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

CVE-2022-22790

SYNEL - eharmony Directory Traversal. Directory Traversal - is an attack against a server or a Web application aimed at unauthorized access to the file system. on the "Name" parameter the attacker can return to the root directory and open the host file. The path exposes sensitive files that users upload

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

CVE-2022-23888

YzmCMS v6.3 was discovered to contain a Cross-Site Request

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

CVE-2021-29845

IBM Security Guardium Insights 3.0 could allow an authenticated user to perform unauthorized actions due to improper input validation. IBM X-Force ID: 205255.

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

CVE-2021-46118

jpress 4.2.0 is vulnerable to remote code execution via io.jpress.module.article.kit.ArticleNotifyKit#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: 2022-02-02

CVE-2020-28885

Liferay Portal Server tested **on 7**.3.5 GA6, 7.2.0 GA1 is affected by OS Command Injection. An administrator user can inject commands through the Gogo Shell module to execute any OS command on the **Liferay Portal** Sever.

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

CVE-2021-22570

Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.

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

CVE-2022-0368

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

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

CVE-2021-42631

PrinterLogic Web Stack versions 19.1.1.13 SP9 and below deserializes attacker controlled leading to pre-auth remote code execution.

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

CVE-2021-42635

PrinterLogic Web Stack versions 19.1.1.13 SP9 and below use a hardcoded APP_KEY value, leading to pre-auth remote code execution.

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

CVE-2021-44793

Single **Connect** does not perform an authorization check when using the sc-reports-ui" module. A remote attacker could exploit this vulnerability to access the device configuration page and export the data to an external file. The exploitation of this vulnerability might allow a remote attacker to obtain sensitive information including the database credentials. Since the database runs with high privileges it is possible to execute commands with the attained credentials.

HIGH Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2021-44123

SPIP 4.0.0 is affected by a remote command execution vulnerability. To exploit the vulnerability, an attacker must craft a malicious picture with a double extension, upload it and then click on it to execute it.

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

CVE-2022-23181

The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into **Apache Tomcat** 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9.0.35 to 9.0.56 and 8.5.55 to 8.5.73 that allowed a local attacker to perform actions with the privileges of the user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore.

HIGH Vector: local Created: 2022-01-27 Updated: 2022-02-02

CVE-2021-46088

Zabbix 4.0 LTS, 4.2, 4.4, and 5.0 LTS is vulnerable to Remote

Forgey (CSRF) via the component /yzmcms/comment/index/init.html.

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

Code Execution (RCE). Any user with the "Zabbix Admin" role is able to run custom shell script on the **application server** in the context of the application user.

HIGH Vector: network Created: 2022-01-27 Updated: 2022-02-02

Source: NIST

NIST CVE: Medium

CVE-2022-24071

A Built-in extension in **Whale** browser before 3.12.129.46 allows attackers to compromise the rendering process which could lead to controlling browser internal APIs.

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

CVE-2021-34073

A Cross Site Scripting (XSS) vulnerabilty exists in **Sourcecodester** Gadget **Works** Online Ordering System in PHP/MySQLi 1.0 via the Category parameter in an add function in category/index.php.

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

CVE-2021-46447

A cross-site scripting (XSS) vulnerability in H.H.G Multistore v5.1.0 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the State parameter under the Address Book module.

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

CVE-2021-46065

A Cross-site scripting (XSS) vulnerability in Secondary Email Field in **Zoho ManageEngine ServiceDesk Plus** 11.3 Build 11306 allows an attackers to inject arbitrary JavaScript code.

MEDIUM Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2021-22809

A CWE-125:Out-of-Bounds Read vulnerability exists that could cause unintended data disclosure when a malicious *.gd1 configuration file is loaded into the **GUIcon** tool. Affected Product: Eurotherm by Schneider Electric GUIcon Version 2.0 (Build 683.003) and prior

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

CVE-2021-26264

A specially crafted script could cause the **DeltaV** Distributed Control System Controllers (All Versions) to restart and cause a denial-of-service condition.

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

CVE-2022-22852

A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodtester Hospital's Patient Records Management System 1.0 via the description parameter in room_list.

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

CVE-2022-22850

A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodtester Hospital's Patient Records Management System 1.0 via the description parameter in room_types.

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

CVE-2021-23174

Authenticated (admin+) Persistent Cross-Site Scripting (XSS) vulnerability discovered in **Download Monitor WordPress** plugin (versions <= 4.4.6) Vulnerable parameters: &post_title, &downloadable_file_version[0].

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

CVE-2022-23979

Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability discovered in **Ultimate Reviews WordPress** plugin (versions <= 3.0.15).

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

CVE-2021-44692

BuddyBoss Platform through 1.8.0 allows remote attackers to obtain the email address of each user. When creating a new user, it generates a Unique ID for their profile. This UID is their private email address with symbols removed and periods replaced with hyphens. For example. JohnDoe@example.com would become /members/johndoeexample-com and Jo.test@example.com would become /members/jo-testexample-com. The members list is available to everyone and (in a default configuration) often without authentication. It is therefore trivial to collect a list of email addresses.

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

CVE-2021-43334

BuddyBoss Platform through 1.8.0 allows XSS via the Group Name or Group Description field.

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

CVE-2022-0378

Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11.

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

CVE-2022-0352

Cross-site Scripting (XSS) - Reflected in **Pypi** calibreweb prior to 0.6.16.

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

CVE-2022-0372

Cross-site Scripting (XSS) - Stored in Packagist bytefury/crater prior to 6.0.2.

MEDIUM Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2022-0379

Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11.

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

CVE-2022-0348

Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.2.

MEDIUM Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2022-0387

Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.

MEDIUM Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2022-0370

Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.

MEDIUM Vector: network Created: 2022-01-27 Updated: 2022-02-02

CVE-2022-0394

Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.

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

CVE-2022-0395

Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.

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

CVE-2022-22868

Gibbon CMS v22.0.01 was discovered to contain a cross-site scripting (XSS) vulnerability, that allows attackers to inject arbitrary script via name parameters.

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

CVE-2022-21719

GLPI is a free asset and IT management software package. All

CVE-2022-21720

GLPI is a free asset and IT management software package. Prior to version 9.5.7, an entity administrator is capable of retrieving

GLPI versions prior to 9.5.7 are vulnerable to reflected cross-site scripting. Version 9.5.7 contains a patch for this issue. There are no known workarounds.

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

normally inaccessible data via SQL injection. Version 9.5.7 contains a patch for this issue. As a workaround, disabling the `Entities` update right prevents exploitation of this vulnerability.

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

CVE-2021-23863

HTML code injection vulnerability in **Android** Application, **Bosch** Video Security, version 3.2.3. or earlier, when successfully exploited allows an attacker to inject random HTML code into a component loaded by WebView, thus allowing the Application to display web **resources** controlled by the attacker.

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

CVE-2021-29838

IBM Security Guardium Insights 3.0 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.

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

CVE-2022-0203

Improper Access Control in **GitHub** repository crater-invoice/crater prior to 6.0.2.

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

CVE-2021-46502

Jsish v3.5.0 was discovered to contain a heap-use-after-free via /usr/lib/x86_64-linux-gnu/libasan.so.4+0x5166d. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46503

Jsish v3.5.0 was discovered to contain a heap-use-after-free via /usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46495

Jsish v3.5.0 was discovered to contain a heap-use-after-free via DeleteTreeValue in src/jsiObj.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46500

Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_ArgTypeCheck in src/jsiFunc.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46489

Jsish v3.5.0 was discovered to contain a heap-use-after-free via Jsi_DecrRefCount in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46484

Jsish v3.5.0 was discovered to contain a heap-use-after-free via Jsi_IncrRefCount in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46496

Jsish v3.5.0 was discovered to contain a heap-use-after-free via Jsi_ObjFree in src/jsiObj.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46497

Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_UserObjDelete in src/jsiUserObj.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46499

Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_ValueCopyMove in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46494

Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_ValueLookupBase in src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46498

Jsish v3.5.0 was discovered to contain a heap-use-after-free via jsi_wswebsocketObjFree in src/jsiWebSocket.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46501

Jsish v3.5.0 was discovered to contain a heap-use-after-free via SortSubCmd in src/jsiArray.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46487

Jsish v3.5.0 was discovered to contain a SEGV vulnerability via /lib/x86_64-linux-gnu/libc.so.6+0x18e506. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46488

Jsish v3.5.0 was discovered to contain a SEGV vulnerability via jsi_ArrayConcatCmd at src/jsiArray.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46486

Jsish v3.5.0 was discovered to contain a SEGV vulnerability via jsi_ArraySpliceCmd at src/jsiArray.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46491

Jsish v3.5.0 was discovered to contain a SEGV vulnerability via Jsi_CommandPkgOpts at src/jsiCmds.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46492

Jsish v3.5.0 was discovered to contain a SEGV vulnerability via Jsi_FunctionInvoke at src/jsiFunc.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46485

Jsish v3.5.0 was discovered to contain a SEGV vulnerability via Jsi_ValueIsNumber at src/jsiValue.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46490

Jsish v3.5.0 was discovered to contain a SEGV vulnerability via NumberConstructor at src/jsiNumber.c. This vulnerability can lead to a Denial of Service (DoS).

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

CVE-2021-46505

Jsish v3.5.0 was discovered to contain a stack overflow via /usr/lib/x86_64-linux-gnu/libasan.so.4+0x5b1e5.

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

CVE-2021-46507

Jsish v3.5.0 was discovered to contain a stack overflow via Jsi_LogMsg at src/jsiUtils.c.

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

CVE-2021-44792

Single **Connect** does not perform an authorization check when using the "log-monitor" module. A remote attacker could exploit this vulnerability to access the logging interface. The exploitation of this vulnerability might allow a remote attacker to obtain sensitive information.

MEDIUM | Vector: network | Created: 2022-01-27 | Updated: 2022-02-02

CVE-2021-44794

Single **Connect** does not perform an authorization check when using the "sc-diagnostic-ui" module. A remote attacker could exploit this vulnerability to access the device information page. The exploitation of this vulnerability might allow a remote attacker to obtain sensitive information.

MEDIUM | Vector: network | Created: 2022-01-27 | Updated: 2022-02-02

CVE-2021-41166

The **Nextcloud Android** app is the Android client for Nextcloud, a self-hosted productivity platform. An issue in versions prior to 3.17.1 may lead to sensitive information disclosure. An unauthorized app that does not have the otherwise required

CVE-2022-22791

SYNEL - eharmony Authenticated Blind & Stored XSS. Inject JS code into the "comments" field could lead to potential stealing of

cookies, loading of HTML tags and JS code onto the system.

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

`MANAGE_DOCUMENTS` permission may view image thumbnails for images it does not have permission to view. Version 3.17.1 contains a patch. There are no known workarounds.

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

CVE-2021-46508 There is an Assertion `i < parts_cnt' failed at src/mjs_bcode.c in **Cesanta** MJS v2.20.0.

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

CVE-2021-46511 There is an Assertion `m->len >= sizeof(v)' failed at src/mjs_core.c in **Cesanta** MJS v2.20.0.

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

CVE-2021-46517 There is an Assertion `mjs_stack_size(&mjs->scopes) > 0' failed at src/mjs_exec.c in **Cesanta** MJS v2.20.0.

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

CVE-2021-46515 There is an Assertion `mjs_stack_size(&mjs->scopes) >= scopes_len' failed at src/mjs_exec.c in **Cesanta** MJS v2.20.0.

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

CVE-2021-46514 There is an Assertion 'ppos != NULL && mjs_is_number(*ppos)' failed at src/mjs_core.c in **Cesanta** MJS v2.20.0.

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

CVE-2021-46504 There is an Assertion 'vp != resPtr' failed at jsiEval.c in **Jsish** v3.5.0.

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

CVE-2022-23887 **YzmCMS** v6.3 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily delete user accounts via /admin/admin_manage/delete.

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

CVE-2022-23863 **Zoho ManageEngine** Desktop **Central** before 10.1.2137.10 allows an authenticated user to change any user's login password.

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

Source: NIST

NIST CVE: Low

CVE-2021-29846 **IBM Security Guardium** Insights 3.0 could allow an authenticated user to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 205256.

LOW Vector: network Created: 2022-01-26 Updated: 2022-02-02

Source: NIST

NIST CVE: Unrated

CVE-2021-43062 A improper neutralization of input during web page generation ('cross-site scripting') in **Fortinet FortiMail** version 7.0.1 and 7.0.0, version 6.4.5 and below, version 6.3.7 and below, version 6.0.11 and below allows attacker to execute unauthorized code or commands via crafted HTTP GET requests to the **FortiGuard** URI protection service.

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

CVE-2021-41016 A improper neutralization of special elements used in a command ('command injection') in **Fortinet FortiExtender** version 7.0.1 and below, 4.2.3 and below, 4.1.7 and below allows an authenticated attacker to execute privileged shell commands via CLI commands including special characters

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

CVE-2021-43073 A improper neutralization of special elements used in an os command ('os command injection') in **Fortinet FortiWeb** version 6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests.

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

CVE-2021-41018 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.

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

CVE-2021-24043 A missing bound check in RTCP flag parsing code prior to **WhatsApp** for **Android** v2.21.23.2, **WhatsApp Business** for Android v2.21.23.2, WhatsApp for iOS v2.21.230.6, WhatsApp Business for iOS 2.21.230.7, and WhatsApp Desktop v2.2145.0 could have allowed an out-of-bounds heap read if a user sent a malformed RTCP packet during an established call.

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

CVE-2022-0366 An authenticated and authorized agent user could potentially gain administrative access via an SQLi vulnerability to Capsule8 Console between versions 4.6.0 and 4.9.1.

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

CVE-2021-36177 An improper access control vulnerability [CWE-284] in **FortiAuthenticator** HA service 6.3.2 and below, 6.2.x, 6.1.x, 6.0.x may allow an attacker on the same vlan as the HA management interface to make an unauthenticated direct connection to the FAC's database.

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

CVE-2021-42753 An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in **FortiWeb** management interface 6.4.1 and below, 6.3.15 and below, 6.2.x, 6.1.x, 6.0.x, 5.9.x and 5.8.x may allow an authenticated attacker to perform an arbitrary file and directory deletion in the device filesystem.

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

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: 2022-02-02

CVE-2021-39066 **IBM Financial Transaction Manager** 3.2.4 does not invalidate session any existing session identifier gives an attacker the opportunity to steal authenticated sessions. IBM X-Force ID: 215040.

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

CVE-2021-39044 **IBM Financial Transaction Manager** 3.2.4 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a

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

user that the website trusts. IBM X-Force ID: 214210.

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

CVE-2021-39070 **IBM Security Verify Access** 10.0.0.0, 10.0.1.0 and 10.0.2.0 with the advanced access control **authentication service** enabled could allow an attacker to **authenticate** as any user on the system. IBM X-Force ID: 215353.

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

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: 2022-02-02

CVE-2022-24198 **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.

UNRATED Vector: unkown Created: 2022-02-01 Updated: 2022-02-02

CVE-2020-26208 **JHEAD** is a simple command line tool for displaying and some manipulation of **EXIF** header data embedded in **Jpeg** images from digital cameras. In affected versions there is a heap-buffer-overflow on jhead-3.04/jpgfile.c:285 ReadJpegSections. Crafted jpeg images can be provided to the user resulting in a program crash or potentially incorrect exif information retrieval. Users are advised to upgrade. There is no known workaround for this issue.

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

CVE-2021-36193 Multiple stack-based buffer overflows in the command line interpreter of **FortiWeb** before 6.4.2 may allow an authenticated attacker to achieve arbitrary code execution via specially crafted commands.

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

CVE-2022-21724 pgjdbc is the offical **PostgreSQL** JDBC Driver. A security hole was found in the jdbc driver for postgresql database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnameverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to remote code execution loaded via arbitrary classes. Users using **plugins** are advised to upgrade. There are no known workarounds for this issue.

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

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: 2022-02-02

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: 2022-02-02

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: 2022-02-02

CVE-2022-0443 Use After Free in Conda vim prior to 8.2.

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

ID: 213856.

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

CVE-2022-24301 In Minetest before 5.4.0, players can add or subtract items from a different player's **inventory**.

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

CVE-2022-24197 **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.

UNRATED Vector: unkown Created: 2022-02-01 Updated: 2022-02-02

CVE-2022-24196 **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.

UNRATED Vector: unkown Created: 2022-02-01 Updated: 2022-02-02

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.

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

CVE-2022-0419 NULL Pointer Dereference in **GitHub** repository radareorg/radare2 prior to 6.0.0.

UNRATED Vector: unkown Created: 2022-02-01 Updated: 2022-02-02

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: 2022-02-02

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: 2022-02-02

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: 2022-02-02

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

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

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 countries with botnet

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

Source: SpamHaus

Top phishing countries

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

Source: Hybrid Analysis

Top malicious files

100% Threat score	tmpwp8yl8r0	100% Threat score	tmpr4ji0x1c
100% Threat score	tmp4dfyoa_s	100% Threat score	tmpue5vgkvm
100% Threat score	tmpdnoqn044	100% Threat score	tmpeu86b5ye
100% Threat score	tmpe7r66fr7	100% Threat score	tmpyh7u_fyi
100% Threat score	tmprxm2h8_5	100% Threat score	tmpkhtp6wfq
100% Threat score	tmpehp3ie9v	100% Threat score	tmp5o3ut55e
100% Threat score	tmplqy8vp8k	100% Threat score	LockDownBrowser-2-0-8-03 . exe
100% Threat score	tmpw9xtgr_c	100% Threat score	tmpsh2vr47f
100% Threat score	tmpg6tdqkcu	100% Threat score	test . doc
100%	TKD 78 . xlsm	100%	Report . xls

Threat score		Threat score	
100%	tmp31m1mw4g	100%	rmm-ablebabelson-joeysbbqbones-server . exe
100%	tmp04j8zmza	100%	hotelwarner . com . xls
100%	DAMsetup . exe	98%	2022-02-03_0951 . xlsm
90%	tmpq5i3s6sm	86%	tmpx_ns9uhf
85%	idasetup . exe	75%	FACTURA-50199 . msi

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: Hybrid Analysis

Top malicious URL

Threat score		Threat score	
100%	http://125 . 47 . 61 . 137:60235/i	100%	http://112 . 95 . 10 . 183:48671/Mozi . a
100%	http://bluebirdgroup . ca/document/contra . php	100%	http://wildcard . dpschool . io/
100%	http://123 . 10 . 184 . 9:56713/Mozi . m	95%	http://www . consultoreimoveis . com . br/
88%	https://pinkelephantlabs . com/show%20you?i=i&0=charisya . handoyo%40one-line . com	82%	https://bit . ly/3EWp2Iq
82%	http://app4u . top/	77%	http://www . ozak . co/
77%	http://taaa0d . quecostuma . us/22ASRIURE844/V472895SSFHJLWR5TU59KDQU241OIP/67956707	77%	http://villepropre-admin . epitech . bj/
77%	http://www . agendaself . com/	77%	http://www . amoradenizcilik . com/
77%	http://bluebirdgroup . ca/	77%	https://gosling . website/COPYRIGHT/assets/images/tech/DPF/intimacao/info/65998599632021/?hash=jessesantos%40mpf . mp . br
77%	http://87a880 . phxxqmwnxjbtq . com/	72%	http://www . blueghost . co/

72%
Threat score

http://taaa0d . quecostuma . us/

72%
Threat score

http://etaa61 . encargojuridico . one/