



Your Security Rabbits report for February 01, 2022

Hot topics

Nothing today

Twitter



Cyber
Advising

CVE-2022-0332: Moodle 3.11 to 3.11.4 - SQL injection PoC



numan
turle

CVE-2022-0332 Moodle 3.11 to 3.11.4 - SQL injection



CORIZANCE
- Connected
Risk
Intelligence

numanturle/CVE-2022-0332 #Cybersecurity
#infosec #security



Evren

Moodle bilmeyen biri olarak setup' hazrlamak baya uzun srd. Tebrikler Numan. CVE-2022-0332



blueblue

GitHub - numanturle/CVE-2022-0332 -



Open
Source
Security

CVE-2022-23944: Apache ShenYu 2.4.1 Improper access control: Posted by Zhang Yonglun on Jan 25
Description: User can access /plugin api without authentication. This issue affected Apache ShenYu 2.4.0 and 2.4.1.



Ptrace
Security
GmbH

CVE-2022-0332 #Pentesting #CVE #CyberSecurity
#Infosec



cckuailong

#nuclei Here is my nuclei template for CVE-2022-23944. Enjoy it! I also make some vuln app and pocs on #reapoc



cckuailong

#CVE CVE-2022-23944 Poc && Vuln App User can access /plugin api without authentication. This issue affected Apache ShenYu 2.4.0 and 2.4.1.



Robo
Shadow
Alerts

Potentially Critical CVE Detected! CVE-2022-0332
Description: A flaw was found in Moodle in versions 3.11 to 3.11.4. An SQL injection risk was... CVSS: 8.68 #moodle #moodle #CVE #CyberSecurity #DataBreach



Prophaze
Web
Security
Platform

Moxa TN-5900 up to 3.1 command injection [CVE-2021-46560] #Exploit:No #Local:No #Product:TN-5900 #Remote:Partially



HackGit

CVE-2022-0332 Moodle 3.11 to 3.11.4 - SQL injection
GitHub - numanturle/CVE-2022-0332 - GitHub
Contribute to numanturle/CVE-2022-0332 development by creating an account on GitHub.

News



'White Tur' Hacking Group Borrows Techniques From Multiple APTs



IT Security
Guru

\$2m Bug Bounty offered to Hackers

Qubit Finance revealed last week that attackers exploited a vulnerability in its QBridge deposit function, resulting in a loss of \$80m. The hackers stole a large amount of Ethereum by converting it

A newly detailed threat actor has been observed employing various techniques borrowed from multiple advanced persistent threat (APT) actors, PwC's cyber threat intelligence team reports.

into Binance coins and exploiting the vulnerability to withdraw the Binance tokens without depositing any of the Ethereum. Qubit has addressed the attackers [...] The post \$2m Bug Bounty offered to Hackers appeared first on IT Security Guru.



A cyber attack severely impacted the operations of German petrol distributor Oiltanking GmbH
German petrol distributor Oiltanking GmbH was a victim of a cyberattack that has a severe impact on its operations. A cyber attack hit Oiltanking GmbH, a German petrol distributor who supplies Shell gas stations in the country, severely impacting its operations. According to the media, the attack also impacted the oil supplier Mabanaft GmbH. The [...] The post A cyber attack severely impacted the operations of German petrol distributor Oiltanking GmbH appeared first on Security Affairs.



Andreas Deliandreadis announced as Kiteworks VP of Sales, EMEA

Kiteworks has announced the appointment of Andreas Deliandreadis as its new Vice President of Sales, EMEA. With more than 20 years in technology and cybersecurity sales and business development in EMEA markets, Deliandreadis is responsible for driving international revenue growth across Europe, the Middle East, and Africa (EMEA). "It is a great honour and privilege [...] The post Andreas Deliandreadis announced as Kiteworks VP of Sales, EMEA appeared first on IT Security Guru.



Apple Pays \$100,500 Bounty to Hacker Who Found Way to Hack MacBook Webcam
Apple last year fixed a new set of macOS vulnerabilities that exposed Safari browser to attack, potentially allowing malicious actors to access users' online accounts, microphone, and webcam. Security researcher Ryan Pickren, who discovered and reported the bugs to the iPhone maker, was compensated with a \$100,500 bug bounty, underscoring the severity of the issues. By exploiting a chain of



Armis and Eseye joint solution reliably secures connected devices on cellular networks

Global connectivity specialist Eseye and agentless device security platform provider, Armis, have announced the general availability of a joint solution that enables organisations to deploy connected devices anywhere in the world with enterprise-class security and consistent, reliable cellular (4G/LTE/5G) connectivity. The joint solution addresses how digital transformation has created a new generation of connected [...] The post Armis and Eseye joint solution reliably secures connected devices on cellular networks appeared first on IT Security Guru.



Behind The Buzzword: Four Ways to Assess Your Zero Trust Security Posture
With just about everything delivered from the cloud these days, employees can now collaborate and access what they need from anywhere and on any device. While this newfound flexibility has changed the way we think about productivity, it has also created new cybersecurity challenges for organizations. Historically, enterprise data was stored inside data centers and guarded by perimeter-based



BlackCat Ransomware Soars to the Top

BlackCat RaaS, also known as ALPHV, first came to light in mid-November and already proved its sophistication. It became the first professional ransomware gang to use Rust-based malware. In less than a month, the gang has amassed more than a dozen victims located in the U.S., Germany, the Netherlands, France, Spain, and the Philippines.



British Council exposed 144,000 files containing student details
Personal information belonging to British Council students was exposed online via an unsecured repository. The British Council is a British organisation specialising in international cultural and educational opportunities. It operates in over 100 countries: promoting a wider knowledge of the United Kingdom and the English language; encouraging cultural, scientific, technological and educational co-operation with the [...] The post British Council exposed 144,000 files containing student details appeared first on Security Affairs.



British Council Exposed More Than 100,000 Files via Unsecured Microsoft Azure Blob

British Council, the global organization for promoting British culture, the English language, and education opportunities, was leaking over 144,000 files containing student records.



CISA adds 8 new vulnerabilities to its Known Exploited Vulnerabilities Catalog
The US CISA added eight more flaws to its Known Exploited Vulnerabilities Catalog that are known to be used in attacks in the wild. The US Cybersecurity & Infrastructure Security Agency (CISA) has added eight more flaws to the Known Exploited Vulnerabilities Catalog. The 'Known



Conversation with a top Ukrainian cyber official: What we know, what we don't, what it means
Cybersecurity officials in Ukraine issued a warning Monday about yet another phishing attack using either compromised or spoofed government email addresses, the second such warning since Saturday. Monday's alert warned of attackers targeting government institutions with malware-laced bait documents hosted on Discord that come to targets within emails from the National Health Service of Ukraine. The malware

Exploited Vulnerabilities Catalog' is a list of known vulnerabilities that [...] The post CISA adds 8 new vulnerabilities to its Known Exploited Vulnerabilities Catalog appeared first on Security Affairs.

deploys a program called OutSteel that looks for certain file extensions and steals them, and also deploys a second malicious program called SaintBot. Monday's bulletin comes two days after government officials there warned of compromised email accounts from the Ukrainian judiciary being u[...]



IT Security
Guru

Cyber attacks at an all time high for UK corps

A new survey of 450 top finance and risk professionals at UK-listed companies have found that nearly two-thirds of organisations have experienced a data breach or cyber attack in the first year and a half of the pandemic. The research also found that the rise in cyber attacks led to the loss of money and [...] The post Cyber attacks at an all time high for UK corps appeared first on IT Security Guru.



Security
Affairs

DeepDotWeb admin sentenced to 97 months in prison for money laundering scheme

The administrator of the DeepDotWeb (DDW) has received a sentence of 97 months in prison for money laundering. Tal Prihar (37), an Israeli national who operated DeepDotWeb (DDW), was sentenced to 97 months in prison and was ordered to forfeit \$8,414,173. DeepDotWeb (DDW) was a website that connected internet users with Darknet marketplaces, where they [...] The post DeepDotWeb admin sentenced to 97 months in prison for money laundering scheme appeared first on Security Affairs.

The Hacker News

The Hacker
News

DeepDotWeb News Site Operator Sentenced to 8 Years for Money Laundering

An Israeli national was sentenced to 97 months in prison in connection with operating the DeepDotWeb (DDW) clearnet website, nearly a year after the individual pleaded guilty to the charges. Tal Prihar, 37, an Israeli citizen residing in Brazil, is said to have played the role of an administrator of DDW since the website became functional in October 2013. He pleaded guilty to money laundering



Security
Affairs

Expert earned \$100,500 bounty to hack Apple MacBook webcam and microphone

Apple paid +\$100K bounty for a macOS series of flaws that can allow threat actors to take over the microphone and camera. Apple last year addressed multiple macOS vulnerabilities discovered by the security researcher Ryan Pickren in the Safari browser that could allow threat actors to access users' online accounts, microphone, and webcam. Pickren received [...] The post Expert earned \$100,500 bounty to hack Apple MacBook webcam and microphone appeared first on Security Affairs.



Cyware
News -
Latest Cyber
News

FBI Issues Warning about Iranian Cyber Firm Emennet

The agency stated that Emennet performed conventional cyber exploitation against news, travel, shipping, financial, telecoms, and oil & petrochemical sectors in the U.S., the Middle East, and Europe.



IT Security
Guru

FBI warn olympians to leave devices at home

The FBI has sent out an alert to warn attendees and athletes going to the Beijing Winter Olympics to leave mobiles and other devices at home due to the risk of potential cybercrime activities at the event. The alert was published yesterday by US law enforcement, who claimed that although they are not aware of [...] The post FBI warn olympians to leave devices at home appeared first on IT Security Guru.



CyberScoop

Forescout acquires medical IoT security company CyberMDX

Silicon Valley cybersecurity company Forescout Technologies said Tuesday that it is acquiring CyberMDX, a medical-device security company known for its research into potential cyberthreats against health care technology. CyberMDX is a natural fit for Forescout, which focuses on securing connected devices and operational technology (OT) for large organizations -- including what the industry calls the Internet of Medical Things (IoMT). Terms of the deal were not disclosed. "Cybersecurity for IoMT, much like cybersecurity for OT devices, requires specific expertise and technologies," Forescout CEO Wael Mohamed said. "We are pleased to have the CyberMDX team join Forescout as we continue deliver[...]



The Hacker
News

German Court Rules Websites Embedding Google Fonts Violates GDPR

A regional court in the German city of Munich has ordered a website operator to pay EUR100 in damages for transferring a user's personal data -- i.e., IP address -- to Google via the search giant's Fonts library without the individual's consent. The unauthorized disclosure of the plaintiff's IP address by the unnamed website to Google constitutes a contravention of the user's privacy rights, the



IT Security
Guru

Hackers are now using ransomware in attempt to remain undetected

Iranian hackers are now using new malware to conduct cyber espionage campaigns and steal data. In some cases they drop ransomware in an attempt to avoid detection. Researchers at



Security
Affairs

Hackers stole \$80M worth of cryptocurrency from the Qubit DeFi platform

Threat actors stole \$80M worth of cryptocurrency from the Qubit DeFi platform by exploiting a flaw in the smart contract code used in an Ethereum bridge. The DeFi platform Qubit Finance was

Cybereason attribute the two separate campaigns to an Iranian hacking group known as Phosphorous. Moses Staff, another state-backed group, is also believed to be involved. It [...] The post Hackers are now using ransomware in attempt to remain undetected appeared first on IT Security Guru.

victim of a cyber heist, threat actors stole around \$80 million in cryptocurrency last week. The hack took place at around 5PM ET [...] The post Hackers stole \$80M worth of cryptocurrency from the Qubit DeFi platform appeared first on Security Affairs.



Security
Affairs

Hundreds of thousands of routers exposed to Eternal Silence campaign via UPnP

A hacking campaign, tracked as Eternal Silence, is abusing UPnP to compromise routers and use them to carry out malicious activities. Researchers from Akamai have spotted a malicious campaign, tracked as 'Eternal Silence,' that is abusing Universal Plug and Play (UPnP) to turn routers into a proxy server used to carry out a broad range [...] The post Hundreds of thousands of routers exposed to Eternal Silence campaign via UPnP appeared first on Security Affairs.



Cyware
News -
Latest Cyber
News

Industrial Firms Under Attack via Short-Lived Campaigns

Kaspersky uncovered short-lived spyware attack campaigns by major infamous malware families, wherein criminals managed to steal over 7000 corporate credentials on ICS networks. Attackers also used the stolen data from corporate networks to perform financial fraud or sell the obtained RDP, SSH, VPN, and SMTP credentials online. Organizations can protect themselves by training employees to identify phishing emails, limiting access, and making 2FA mandatory.



Security
Affairs

Iran-linked MuddyWater APT group campaign targets Turkish entities

The Iran-linked MuddyWater APT group is targeting private Turkish organizations and governmental institutions. Researchers from Cisco Talos have uncovered a cyber espionage campaign carried out by the Iran-linked MuddyWater APT group (aka SeedWorm and TEMP.Zagros) and targeting private Turkish organizations and governmental institutions. The first MuddyWater campaign was observed in late 2017 when targeted entities in the Middle East. The experts called the [...] The post Iran-linked MuddyWater APT group campaign targets Turkish entities appeared first on Security Affairs.



The Hacker
News

Iranian Hackers Using New PowerShell Backdoor in Cyber Espionage Attacks

An advanced persistent threat group with links to Iran has updated its malware toolset to include a novel PowerShell-based implant called PowerLess Backdoor, according to new research published by Cybereason. The Boston-headquartered cybersecurity company attributed the malware to a hacking group known as Charming Kitten (aka Phosphorous, APT35, or TA453), while also calling out the backdoor's



Cyware
News -
Latest Cyber
News

Iranian Hackers Using New PowerShell-based Backdoor in Cyber Espionage Attacks

An APT group with links to Iran has updated its malware toolset to include a novel PowerShell-based implant called PowerLess Backdoor, according to new research published by Cybereason.



Naked
Security

Linux kernel patches "performance can be harmful" bug in video driver

This bug is fiendishly hard to exploit - but if you patch, it won't be there to exploit at all.



CyberScoop

Major German fuel storage provider hit with cyberattack, working under limited operations

A cyberattack struck major German oil storage company Oiltanking GmbH Group on Sunday, the company confirmed to CyberScoop in a statement. The cyberattack affected the IT systems of Oiltanking as well as the mineral oil trade company Mabanaft, German news outlet Handelsblatt first reported. Both companies belong to the Hamburg-based Marquard & Bahls group, one of the world's largest energy supply companies. The attack shut down the oil tank company's IT systems, according to a statement by the company's head of corporate communications, Claudia Wagner. Oiltanking's German subsidiary which operates all terminals in Germany is operating at limited capacity. Oiltanking's global operations w[...]



Cyware
News -
Latest Cyber
News

Major German Fuel Storage Provider Suffers Cyberattack Impacting IT Systems

A cyberattack struck major German oil storage company Oiltanking GmbH Group on Sunday, the company confirmed to CyberScoop. The attack shut down the oil tank company's IT systems.



Cyware
News -
Latest Cyber
News

Microsoft OneDrive for macOS Local Privilege Escalation

It took Microsoft over a year to fix the vulnerability and the patched version of OneDrive was released in December 2021. A CVE number was not assigned to this vulnerability.



Cyware
News -
Latest Cyber
News

New Hybrid Campaign OiVaVoi Uses Malicious OAuth Apps

OiVaVoi is targeting general managers and company executives with malicious OAuth apps and custom phishing messages sent from hijacked Microsoft Office 365 accounts.

The Hacker News

The Hacker News

New Samba Bug Allows Remote Attackers to Execute Arbitrary Code as Root

Samba has issued software updates to address multiple security vulnerabilities that, if successfully exploited, could allow remote attackers to execute arbitrary code with the highest privileges on affected installations. Chief among them is CVE-2021-44142, which impacts all versions of Samba before 4.13.17 and concerns an out-of-bounds heap read/write vulnerability in the VFS module "vfs_fruit"

threatpost

Threatpost

NSO Group Pegasus Spyware Aims at Finnish Diplomats

Finland is weathering a bout of Pegasus infections, along with a Facebook Messenger phishing scam.

IT SECURITY GURU

IT Security Guru

One in seven ransom extortion attempts leak key operational data

One in seven ransomware extortion data leaks are revealing technology data critical to business operation, researchers say. In recent years, ransomware has catapulted in severity from its early days as barebone encryption and basic demand for payment. Historically, ransomware was used to infect systems and extort payments from the general public, typically in cryptocurrency such [...] The post One in seven ransom extortion attempts leak key operational data appeared first on IT Security Guru.

CYWARE SOCIAL

Cyware News - Latest Cyber News

Organizations neglecting Microsoft 365 cybersecurity features

As per a new survey, 38% are not using Multi-factor Authentication, only 43% are using Conditional Access Controls, and 46% do not have data loss prevention (DLP) or data classification configured.

Security Affairs

Security Affairs

RCE in WordPress plugin Essential Addons for Elementor impacts hundreds of thousands of websites

A critical RCE in the popular WordPress plugin Essential Addons for Elementor impacts hundreds of thousands of websites. Essential Addons for Elementor is a popular WordPress plugin used in over a million sites that provides easy-to-use and creative elements to improve the appearance of the pages. The plugin is affected by a critical remote code [...] The post RCE in WordPress plugin Essential Addons for Elementor impacts hundreds of thousands of websites appeared first on Security Affairs.

cyberscoop

CyberScoop

Researchers detail Russia-linked group's cyber-espionage tactics in Ukraine

Researchers at Symantec say they have identified some of the specific tactics used by a Russia-linked hacking operation that Ukraine's government outed in November of last year. The cyber-espionage group, commonly labeled as Gamaredon or Armageddon, is known for using phishing emails to try to install remote access tools on victims' computers, with the goal of exfiltrating data. Symantec's Threat Hunter Team published a blog post Monday explaining how the spies used infected Microsoft Word attachments in mid-2021 to implant backdoor files allowing for the delivery of more malware. The researchers don't specify who was targeted in their case study. The goal is to highlight the tactics,

The Hacker News

The Hacker News

New SureMDM Vulnerabilities Could Expose Companies to Supply Chain Attacks

A number of security vulnerabilities have been disclosed in 42 Gears' SureMDM device management solution that could be weaponized by attackers to perform a supply chain compromise against affected organizations. Cybersecurity firm Immersive Labs, in a technical write-up detailing the findings, said that 42Gears released a series of updates between November 2021 and January 2022 to close out

CYWARE SOCIAL

Cyware News - Latest Cyber News

Number of COVID-19 Testing Scams Jumps Sharply

The number of COVID-19 test-related phishing scams increased by 521% between October 2021 and January 2022, according to a report published by security firm Barracuda Networks.

ZDNet

ZDNet | security RSS

One in seven ransomware extortion attempts leak key operational tech records

Researchers say that double-extortion ransomware attacks represent a severe risk to operational processes.

threatpost

Threatpost

Public Exploit Released for Windows 10 Bug

The vulnerability affects all unpatched Windows 10 versions following a messy Microsoft January update.

The Hacker News

The Hacker News

Reasons Why Every Business is a Target of DDoS Attacks

DDoS (Distributed Denial of Service) attacks are making headlines almost every day. 2021 saw a 434% upsurge in DDoS attacks, 5.5 times higher than 2020. Q3 2021 saw a 24% increase in the number of DDoS attacks in comparison to Q3 2020. Advanced DDoS attacks that are typically targeted, known as smart attacks, rose by 31% in the same period. Further, 73% of DDoS attacks in Q3 2021 were

The Hacker News

The Hacker News

Researchers Uncover New Iranian Hacking Campaign Targeting Turkish Users

Details have emerged about a previously undocumented malware campaign undertaken by the Iranian MuddyWater advanced persistent threat (APT) group targeting Turkish private organizations and governmental institutions. "This campaign utilizes malicious PDFs, XLS files and Windows executables to deploy malicious PowerShell-based downloaders acting as initial footholds into the target's enterprise,"

techni[...]

The Hacker News

The Hacker
News

Researchers Use Natural Silk Fibers to Generate Secure Keys for Strong Authentication

A group of academics at South Korea's Gwangju Institute of Science and Technology (GIST) have utilized natural silk fibers from domesticated silkworms to build an environmentally friendly digital security system that they say is "practically unbreachable." "The first natural physical unclonable function (PUF) [...] takes advantage of the diffraction of light through natural microholes in native



Security
Affairs

Samba fixed CVE-2021-44142 remote code execution flaw

Samba fixes a critical flaw, tracked as CVE-2021-44142, that can allow remote attackers to execute code with root privileges. Samba has addressed a critical vulnerability, tracked as CVE-2021-44142, that can be exploited by remote attackers to gain code execution with root privileges on servers running vulnerable software. Samba is a free software re-implementation of the SMB networking [...] The post Samba fixed CVE-2021-44142 remote code execution flaw appeared first on Security Affairs.



Threatpost

Samba 'Fruit' Bug Allows RCE, Full Root User Access

The issue in the file-sharing and interop platform also affects Red Hat, SUSE Linux and Ubuntu packages.



IC3.gov
News

Scammers Exploit Security Weaknesses on Job Recruitment Websites to Impersonate Legitimate Businesses, Threatening Company Reputation and Defrauding Job Seekers



Cyware
News -
Latest Cyber
News

Solarmarker Malware Uses Novel Techniques to Persist on Compromised Systems

The operators behind the SolarMarker information stealer and backdoor have been found leveraging stealthy tricks to establish long-term persistence on compromised systems.

The Hacker News

The Hacker
News

SolarMarker Malware Uses Novel Techniques to Persist on Hacked Systems

In a sign that threat actors continuously shift tactics and update their defensive measures, the operators of the SolarMarker information stealer and backdoor have been found leveraging stealthy Windows Registry tricks to establish long-term persistence on compromised systems. Cybersecurity firm Sophos, which spotted the new behavior, said that the remote access implants are still being detected



ZDNet |
security RSS

State-sponsored Iranian hackers attack Turkish government, private organizations

MuddyWater is impersonating the Turkish Health and Interior Ministries to sink its claws into victim networks.



Cyware
News -
Latest Cyber
News

Telco fined \$10.2 million for hiding cyberattack impact to customers

The Greek data protection authority has imposed fines of \$6.55 million to COSMOTEL and \$3.65 million to OTE, for leaking sensitive customer communication due to a cyberattack.



Threatpost

The Account Takeover Cat-and-Mouse Game

ATO attacks are evolving. Jason Kent, hacker-in-residence at Cequence Security, discusses what new-style cyberattacks look like in the wild.



Blog & Flashpoint

The Great Cyber Exit: Why the Number of Illicit Marketplaces Is Dwindling

Shutdowns, takedowns, retirements, and resignations 2021 was a strange year for cybercrime marketplaces-those illicit venues that mimic the e-commerce experience, but for drugs, fraud guides, and other strange oddities and curiosities. While exit scams and sudden closures are ordinarily the norm, this past year was full of planned closures and announced retirements, as well as [...] The post The Great Cyber Exit: Why the Number of Illicit Marketplaces Is Dwindling appeared first on Flashpoint.



CyberScoop

Top White House cyber adviser Anne Neuberger makes the rounds in Europe

A top U.S. cyber official is in Europe this week to "elevate cybersecurity as a top-tier priority at NATO and with international partners," a senior Biden administration official told reporters Tuesday morning. Anne Neuberger, the deputy national security adviser for cyber and emerging technology, starts her trip in Brussels to meet with counterparts at NATO and the European



Cyware
News -

Top-Ranking Ramnit Banking Trojan Looking to Steal Payment Card Data

Not only was Ramnit the top active banking trojan in 2021, but it has also been a cybercrime tool for over a decade. It continues to target people and

Union to discuss "detering, disrupting, and responding to further Russian aggression against Ukraine, neighboring states, and in our respective countries," the official said. Neuberger also will make a stop in Warsaw to meet with Polish and other Baltic region officials. The week also will include "virtual meetings" wit[...]

Latest Cyber
News

service providers in the online shopping season.

The Hacker News

The Hacker
News

Ukraine Continues to Face Cyber Espionage Attacks from Russian Hackers

Cybersecurity researchers on Monday said they uncovered evidence of attempted attacks by a Russia-linked hacking operation targeting a Ukrainian entity in July 2021. Broadcom-owned Symantec, in a new report published Monday, attributed the attacks to an actor tracked as Gamaredon (aka Shuckworm or Armageddon), a cyber-espionage collective known to be active since at least 2013. In November 2021,



Threatpost

Unpatched Security Bugs in Medical Wearables Allow Patient Tracking, Data Theft

Rising critical unpatched vulnerabilities and a lack of encryption leave medical device data defenseless, researcher warn.

ZDNet

ZDNet |
security RSS

Unsecured AWS server exposed 3TB in airport employee records

The exposure impacted airport staff across Colombia and Peru.



Naked
Security

Website operator fined for using Google Fonts "the cloudy way"

Google Fonts are OK, it seems, but only if everyone keeps their own copy of the fonts they use.

The Hacker News

The Hacker
News

Your Graphics Card Fingerprint Can Be Used to Track Your Activities Across the Web

Researchers have demonstrated a new type of fingerprinting technique that exploits a machine's graphics processing unit (GPU) as a means to persistently track users across the web. Dubbed DrawnApart, the method "identifies a device from the unique properties of its GPU stack," researchers from Australia, France, and Israel said in a new paper," adding "variations in speed among the multiple

Source: *NIST*

NIST CVE: Critical

CVE-2022-0332

A flaw was found in **Moodle** in versions 3.11 to 3.11.4. An SQL injection risk was identified in the h5p activity web service responsible for fetching user attempt data.

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

CVE-2021-43298

The code that performs password matching when using 'Basic' HTTP authentication does not use a constant-time memcmp and has no rate-limiting. This means that an unauthenticated network attacker can brute-force the HTTP basic password, byte-by-byte, by recording the webserver's response time until the unauthorized (401) response.

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

CVE-2021-46560

The firmware on **Moxa** TN-5900 devices through 3.1 allows command injection that could lead to device damage.

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

CVE-2022-23944

User can access /plugin api without authentication. This issue affected **Apache** ShenYu 2.4.0 and 2.4.1.

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

Source: *NIST*

NIST CVE: High

CVE-2021-4133

A flaw was found in **Keycloak** in versions from 12.0.0 and before 15.1.1 which allows an attacker with any existing user account to create new default user accounts via the administrative REST API even when new user registration is disabled.

HIGH

Vector:
networkCreated:
2022-01-25Updated:
2022-02-01

CVE-2022-0335

A flaw was found in **Moodle** in versions 3.11 to 3.11.4, 3.10 to 3.10.8, 3.9 to 3.9.11 and earlier unsupported versions. The "delete **badge** alignment" functionality did not include the necessary token check to prevent a CSRF risk.

HIGH

Vector:
networkCreated:
2022-01-25Updated:
2022-02-01

CVE-2021-41598

A UI misrepresentation vulnerability was identified in **GitHub Enterprise Server** that allowed more permissions to be granted during a GitHub App's user-authorization web flow than was displayed to the user during approval. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. All permissions being granted would properly be shown during the **first** authorization, but if the user later updated the set of repositories the app was installed on after the GitHub App had configured additional user-level permissions, those additional permissions would not be displayed, leading to more permissions being granted than the user potentially intended. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.2.5, 3.1.13, 3.0.21. This vulnerability was reported via the GitHub Bug Bounty program.

HIGH

Vector:
networkCreated:
2022-01-25Updated:
2022-02-01

CVE-2022-23033

arm: guest_physmap_remove_page not removing the p2m mappings The functions to remove one or more entries from a guest p2m pagetable on Arm (p2m_remove_mapping, guest_physmap_remove_page, and p2m_set_entry with mfn set to INVALID_MFN) do not actually clear the pagetable entry if the entry doesn't have the valid bit set. It is possible to have a valid pagetable entry without the valid bit set when a guest operating system uses set/way cache maintenance instructions. For instance, a guest issuing a set/way cache maintenance instruction, then calling the XENMEM_decrease_reservation hypercall to give back memory pages to Xen, might be able to retain access to those pages even after Xen started reusing them for other purposes.

HIGH

Vector:
localCreated:
2022-01-25Updated:
2022-02-01

CVE-2022-22789

Charactell - FormStorm Enterprise Account takeover - An attacker can modify (add, remove and update) passwords file for all the users. The xx_users.ini file in the FormStorm folder contains usernames in cleartext and an obfuscated password. Malicious user can take over an account by replacing existing password in the file.

HIGH

Vector:
localCreated:
2022-01-25Updated:
2022-02-01

CVE-2022-0355

Exposure of Sensitive Information to an Unauthorized Actor in NPM simple-get prior to 4.0.1.

HIGH

Vector:
networkCreated:
2022-01-26Updated:
2022-02-01

CVE-2022-21697

Jupyter Server Proxy is a Jupyter **notebook** server extension to proxy web services. Versions of **Jupyter Server** Proxy prior to 3.2.1 are vulnerable to Server-Side Request Forgery (SSRF). Any user deploying Jupyter Server or Notebook with jupyter-proxy-server extension enabled is affected. A lack of input validation allows authenticated clients to proxy requests to other hosts, bypassing the `allowed_hosts` check. Because authentication is required, which already grants permissions to make the same requests via kernel or terminal execution, this is considered low to moderate severity. Users may upgrade to version 3.2.1 to receive a patch or, as a workaround, install the patch manually.

HIGH

Vector:
networkCreated:
2022-01-25Updated:
2022-02-01

CVE-2022-23945

Missing authentication on ShenYu Admin when register by HTTP. This issue affected **Apache** ShenYu 2.4.0 and 2.4.1.

HIGH

Vector:
networkCreated:
2022-01-25Updated:
2022-02-01

CVE-2022-23018

On **BIG-IP** AFM version 16.1.x before 16.1.2, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.5, and 13.1.x beginning in 13.1.3.4, when a **virtual server** is configured with both HTTP protocol security and HTTP Proxy **Connect** profiles,

CVE-2022-23024

On **BIG-IP** AFM version 16.x before 16.1.0, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.2, and all versions of 13.1.x, when the IPsec application layer gateway (ALG) logging profile is configured on an IPsec ALG virtual server, undisclosed IPsec traffic can cause the Traffic

undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23025

On **BIG-IP** version 16.1.x before 16.1.1, 15.1.x before 15.1.4, 14.1.x before 14.1.4.4, and all versions of 13.1.x, when a SIP ALG profile is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23019

On **BIG-IP** version 16.1.x before 16.1.2, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.4, and all versions of 13.1.x and 12.1.x, when a message routing type **virtual server** is configured with both Diameter Session and Router Profiles, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23022

On **BIG-IP** version 16.1.x before 16.1.2, when an HTTP profile is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23021

On **BIG-IP** version 16.1.x before 16.1.2, when any of the following configurations are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate: HTTP redirect rule in an LTM policy, BIG-IP APM Access Profile, and Explicit HTTP Proxy in HTTP Profile. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23020

On **BIG-IP** version 16.1.x before 16.1.2, when the 'Respond on Error' setting is enabled on the Request Logging profile and configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23017

On **BIG-IP** version 16.x before 16.1.0, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.5, and all versions of 13.1.x, when a **virtual server** is configured with a DNS profile with the **Rapid** Response Mode setting enabled and is configured on a BIG-IP system, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23012

On **BIG-IP** versions 15.1.x before 15.1.4.1 and 14.1.x before 14.1.4.5, when the HTTP/2 profile is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23010

On **BIG-IP** versions 16.x before 16.1.0, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.4, and all versions of 13.1.x, 12.1.x, and 11.6.x, when a FastL4 profile and an HTTP profile are configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23015

On **BIG-IP** versions 16.x before 16.1.0, 15.1.x before 15.1.4.1, and 14.1.2.6-14.1.4.4, when a Client SSL profile is configured on a **virtual server** with Client Certificate Authentication set to request/require and Session Ticket enabled and configured, processing SSL traffic can

CVE-2022-23009

On **BIG-IQ Centralized Management** 8.x before 8.1.0, an authenticated administrative role user on a BIG-IQ managed **BIG-IP** device can access other BIG-IP devices managed by the same

cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

BIG-IQ system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23011

On certain hardware **BIG-IP** platforms, in version 15.1.x before 15.1.4 and 14.1.x before 14.1.3, virtual servers may stop responding while processing TCP traffic due to an issue in the SYN **Cookie** Protection feature. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23008

On **NGINX** Controller **API Management** versions 3.18.0-3.19.0, an authenticated attacker with access to the "user" or "admin" role can use undisclosed API endpoints on **NGINX Controller** API Management to inject JavaScript code that is executed on managed NGINX data plane instances. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23016

On versions 16.1.x before 16.1.2 and 15.1.x before 15.1.4.1, when **BIG-IP** SSL Forward Proxy with TLS 1.3 is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-0270

Prior to v0.6.1, bored-agent failed to sanitize incoming **kubernetes** impersonation headers allowing a user to override assigned user name and groups.

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

CVE-2022-23223

The HTTP response will disclose the user password. This issue affected **Apache** ShenYu 2.4.0 and 2.4.1.

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

CVE-2021-45845

The Path Sanity Check script of FreeCAD 0.19 is vulnerable to OS command injection, allowing an attacker to execute arbitrary commands via a crafted FCStd document.

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

CVE-2021-24906

The **Protect** WP Admin **WordPress** plugin before 3.6.2 does not check for authorisation in the lib/pwa-deactivate.php file, which could allow unauthenticated users to disable the plugin (and therefore the protection offered) via a crafted request

HIGH Vector: Created: Updated:
network 2022-01-24 2022-02-01

CVE-2021-34869

This vulnerability allows local attackers to escalate privileges on affected installations of **Parallels** Desktop 16.1.3-49160. An attacker must **first** obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in an uncontrolled memory allocation. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13797.

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

CVE-2021-34865

This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of multiple **NETGEAR** routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the mini_httpd service, which listens on TCP port 80 by default. The issue results from incorrect string matching logic when accessing **protected pages**. An attacker can leverage this vulnerability to escalate

privileges and execute arbitrary code in the context of root. Was ZDI-CAN-13313.

HIGH

Vector:
adjacent_network

Created: Updated:
2022- 2022-02-
01-25 01

Source: *NIST*

NIST CVE: Medium

CVE-2022-0334

A flaw was found in **Moodle** in versions 3.11 to 3.11.4, 3.10 to 3.10.8, 3.9 to 3.9.11 and earlier unsupported versions. Insufficient capability checks could lead to users accessing their grade **report** for courses where they did not have the required gradereport/user:view capability.

MEDIUM

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

CVE-2022-23034

A PV guest could DoS Xen while unmapping a grant To address XSA-380, reference counting was introduced for grant mappings for the case where a PV guest would have the IOMMU enabled. PV guests can request two **forms** of mappings. When both are in use for any individual mapping, unmapping of such a mapping can be requested in two steps. The reference count for such a mapping would then mistakenly be decremented twice. Underflow of the counters gets detected, resulting in the triggering of a hypervisor bug check.

MEDIUM

Vector: Created: Updated:
local 2022-01-25 2022-02-01

CVE-2022-0375

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

MEDIUM

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

CVE-2022-23032

In all versions before 7.2.1.4, when proxy settings are configured in the network access resource of a **BIG-IP** APM system, connecting **BIG-IP Edge** Client on Mac and **Windows** is vulnerable to a DNS rebinding attack. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

MEDIUM

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

CVE-2022-23035

Insufficient cleanup of passed-through device IRQs The management of IRQs associated with physical devices exposed to x86 HVM guests involves an iterative operation in particular when cleaning up after the guest's use of the device. In the case where an interrupt is not quiescent yet at the time this cleanup gets invoked, the cleanup attempt may be scheduled to be retried. When multiple interrupts are involved, this scheduling of a retry may

CVE-2021-4145

A NULL pointer dereference issue was found in the block mirror layer of **QEMU** in versions prior to 6.2.0. The ``self`` pointer is dereferenced in `mirror_wait_on_conflicts()` without ensuring that it's not `NULL`. A malicious unprivileged user within the guest could use this flaw to crash the QEMU process on the host when writing data reaches the threshold of mirroring node.

MEDIUM

Vector: Created: Updated:
local 2022-01-25 2022-02-01

CVE-2022-0251

Cross-site Scripting (XSS) - Stored in **GitHub** repository pimcore/pimcore prior to 10.2.10.

MEDIUM

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

CVE-2022-0374

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

MEDIUM

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

CVE-2019-25056

In Bromite through 78.0.3904.130, there are **adblock** rules in the release APK; therefore, probing which **resources** are blocked and which aren't can identify the application version and defeat the User-Agent protection mechanism.

MEDIUM

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

CVE-2022-23028

On **BIG-IP** AFM version 16.x before 16.1.0, 15.1.x before 15.1.5, 14.1.x before 14.1.4.5, and all versions of 13.1.x, when global AFM SYN **cookie** protection (TCP Half Open flood vector) is activated in the AFM Device Dos or DOS profile, certain types of TCP connections will fail. Note: Software versions which have reached

get erroneously skipped. At the same time pointers may get cleared (resulting in a de-reference of NULL) and freed (resulting in a use-after-free), while other code would continue to assume them to be valid.

MEDIUM Vector: physical Created: 2022-01-25 Updated: 2022-02-01

End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23026

On **BIG-IP** ASM & Advanced WAF version 16.1.x before 16.1.2, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.5, and all versions of 13.1.x and 12.1.x, an authenticated user with low privileges, such as a guest, can upload data using an undisclosed REST **endpoint** causing an increase in disk resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23031

On **BIG-IP** FPS, ASM, and Advanced WAF versions 16.1.x before 16.1.1, 15.1.x before 15.1.4, and 14.1.x before 14.1.4.4, an XML External Entity (XXE) vulnerability exists in an undisclosed page of the F5 Advanced Web Application **Firewall** (Advanced WAF) and BIG-IP ASM Traffic Management User Interface (TMUI), also referred to as the Configuration utility, that allows an authenticated high-privileged attacker to read local files and force BIG-IP to send HTTP requests. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23023

On **BIG-IP** version 16.1.x before 16.1.2.1, 15.1.x before 15.1.5, 14.1.x before 14.1.4.5, and all versions of 13.1.x and 12.1.x, and BIG-IQ all versions of 8.x and 7.x, undisclosed requests by an authenticated iControl REST user can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23029

On **BIG-IP** version 16.x before 16.1.0, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.4, and all versions of 13.1.x, 12.1.x, and 11.6.x, when a FastL4 profile is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23027

On **BIG-IP** versions 15.1.x before 15.1.4, 14.1.x before 14.1.4.4, 13.1.x beginning in 13.1.3.6, 12.1.5.3-12.1.6, and 11.6.5.2, when a FastL4 profile and an HTTP, FIX, and/or hash persistence profile are configured on the same virtual server, undisclosed requests can cause the virtual server to stop processing new client connections. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23030

On version 16.1.x before 16.1.2, 15.1.x before 15.1.4.1, 14.1.x before 14.1.4.5, and all versions of 13.1.x, when the **BIG-IP** Virtual Edition (VE) uses the ixlv driver (which is used in SR-IOV mode and requires **Intel** X710/XL710/XXV710 family of network adapters on the Hypervisor) and TCP Segmentation Offload configuration is enabled, undisclosed requests may cause an increase in CPU resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

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

CVE-2022-23014

On versions 16.1.x before 16.1.2 and 15.1.x before 15.1.4.1, when **BIG-IP** APM **portal** access is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

MEDIUM Vector: Created: Updated:

CVE-2021-44120

SPiP 4.0.0 is affected by a Cross Site Scripting (XSS) vulnerability in `ecrre/public/interfaces.php`, adding the function `safehtml` to the vulnerable fields. An editor is able to modify his **personal** information. If the editor has an article written and available, when a user goes to the public site and wants to read the author's information, the malicious code will be executed. The "Who are you" and "Website Name" fields are vulnerable.

MEDIUM Created:

MEDIUM network 2022-01-25 2022-02-01

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

CVE-2021-44118

SPiP 4.0.0 is affected by a Cross Site Scripting (XSS) vulnerability. To exploit the vulnerability, a visitor must browse to a malicious SVG file. The vulnerability allows an authenticated attacker to inject malicious code running on the client side into web pages visited by other users (stored XSS).

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

CVE-2021-45729

The Privilege Escalation vulnerability discovered in the WP **Google Map WordPress** plugin (versions <= 1.8.0) allows authenticated low-role users to create, edit, and delete maps.

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

CVE-2021-24733

The WP Post Page Clone **WordPress** plugin before 1.2 allows users with a role as low as Contributor to clone and view other users' draft and password-protected posts which they cannot view normally.

MEDIUM Vector: Created: Updated:
network 2022-01-24 2022-02-01

CVE-2022-23437

There's a vulnerability within the **Apache Xerces Java** (XercesJ) **XML parser** when handling specially crafted XML document payloads. This causes, the XercesJ XML parser to wait in an infinite loop, which may sometimes consume system **resources** for prolonged duration. This vulnerability is present within XercesJ version 2.12.1 and the previous versions.

MEDIUM Vector: Created: Updated:
network 2022-01-24 2022-02-01

Source: *NIST*

NIST CVE: Low

CVE-2022-0333

A flaw was found in **Moodle** in versions 3.11 to 3.11.4, 3.10 to 3.10.8, 3.9 to 3.9.11 and earlier unsupported versions. The calendar:manageentries capability allowed managers to access or modify any calendar event, but should have been restricted from accessing user level events.

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

CVE-2021-38129

Escalation of privileges vulnerability in Micro Focus in Micro Focus Operations Agent, affecting versions 12.x up to and including 12.21. The vulnerability could be exploited by a non-privileged local user to access system monitoring data collected by Operations Agent.

LOW Vector: Created: Updated:
local 2022-01-25 2022-02-01

Source: *NIST*

NIST CVE: Unrated

CVE-2021-46253

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

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

CVE-2022-24218

An issue in /admin/delete_image.php of **eliteCMS** v1.0 allows attackers to delete arbitrary files.

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

CVE-2021-44451

Apache Superset up to and including 1.3.2 allowed for registered database connections password leak for authenticated users. This information could be accessed in a non-trivial way. Users should upgrade to Apache Superset 1.4.0 or higher.

CVE-2020-8562

As mitigations to a **report** from 2019 and CVE-2020-8555, **Kubernetes** attempts to prevent proxied connections from accessing link-local or localhost networks when making user-driven connections to Services, Pods, Nodes, or StorageClass service providers. As part of this mitigation Kubernetes does a DNS name resolution check and validates that response IPs are not in the link-local (169.254.0.0/16) or localhost (127.0.0.0/8) range. Kubernetes then performs a second DNS resolution

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

without validation for the actual connection. If a non-standard **DNS server** returns different non-cached responses, a user may be able to bypass the proxy IP restriction and access private networks on the control plane.

UNRATED

Vector:
unkownCreated:
2022-02-01Updated:
2022-02-01

CVE-2022-24223

AtomCMS v2.0 was discovered to contain a SQL injection vulnerability via /admin/login.php.

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

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.

UNRATED

Vector:
unkownCreated:
2022-01-
31Updated:
2022-02-
01

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.

UNRATED

Vector:
unkownCreated:
2022-01-
31Updated:
2022-02-
01

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.

UNRATED

Vector:
unkownCreated:
2022-01-
31Updated:
2022-02-
01

CVE-2022-23774

Docker Desktop before 4.4.4 on **Windows** allows attackers to move arbitrary files.

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

CVE-2022-23597

Element Desktop is a **Matrix** client for desktop platforms with Element Web at its core. Element Desktop before 1.9.7 is vulnerable to a remote program execution bug with user interaction. The exploit is non-trivial and requires clicking on a malicious link, followed by another button click. To the best of our knowledge, the vulnerability has never been exploited in the wild. If you are using Element Desktop < 1.9.7, we recommend upgrading at your earliest convenience. If successfully exploited, the vulnerability allows an attacker to specify a file path of a binary on the victim's computer which then gets executed. Notably, the attacker does **not** have the ability to specify program arguments. However, in certain unspecified configurations, the attacker may be able to specify an URI instead of a file path which then gets handled using **standard** platform mechanisms. These may allow exploiting further vulnerabilities in those mechanisms, potentially leading to arbitrary code execution.

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

CVE-2021-46093

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

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

CVE-2022-24219

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

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

CVE-2022-24220

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

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

CVE-2022-24222

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

UNRATED

Vector:
unkownCreated:
2022-02-
01Updated:
2022-02-
01

CVE-2022-23872

Emlog pro v1.1.1 was discovered to

CVE-2022-24221

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

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

contain a stored cross-site scripting (XSS) vulnerability in the component /admin/configure.php via the parameter footer_info.

UNRATED	Vector: unkown	Created: 2022-01-31	Updated: 2022-02-01
---------	-------------------	------------------------	------------------------

CVE-2022-21687

gh-ost is a triggerless online **schema** migration solution for **MySQL**. Versions prior to 1.1.3 are subject to an arbitrary file read vulnerability. The attacker must have access to the target host or trick an administrator into executing a malicious gh-ost command on a host running gh-ost, **plus** network access from host running gh-ost to the attack's malicious **MySQL server**. The '-database' parameter does not properly sanitize user input which can lead to arbitrary file reads.

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

CVE-2021-43848

h2o is an open source http server. In code prior to the `8c0eca3` commit h2o may attempt to access uninitialized memory. When receiving QUIC frames in certain order, HTTP/3 server-side implementation of h2o can be misguided to treat uninitialized memory as HTTP/3 frames that have been received. When h2o is used as a reverse proxy, an attacker can abuse this vulnerability to send internal state of h2o to backend servers controlled by the attacker or third party. Also, if there is an HTTP **endpoint** that reflects the traffic sent from the client, an attacker can use that reflector to obtain internal state of h2o. This internal state includes traffic of other connections in unencrypted form and TLS session **tickets**. This vulnerability exists in h2o server with HTTP/3 support, between commit 93af138 and d1f0f65. None of the released versions of h2o are affected by this vulnerability. There are no known workarounds. Users of unreleased versions of h2o using HTTP/3 are advised to upgrade immediately.

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

CVE-2022-0417

Heap-based Buffer Overflow in Conda vim prior to 8.2.

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

CVE-2022-24263

Hospital Management System v4.0 was discovered to contain a SQL injection vulnerability in /Hospital-Management-System-master/func.php via the email parameter.

UNRATED	Vector: unkown	Created: 2022-01-31	Updated: 2022-02-01
---------	-------------------	------------------------	------------------------

CVE-2021-41571

In **Apache Pulsar** it is possible to access data from BookKeeper that does not belong to the topics accessible by the authenticated user. The Admin API get-message-by-id requires the user to input a topic and a **ledger** id. The ledger id is a pointer to the data, and it is supposed to be a valid id for the topic. Authorisation controls are performed against the topic name and there is not proper validation the that ledger id is valid in the context of such ledger. So it may happen that the user is able to read from a ledger that contains data owned by another tenant. This issue affects Apache Pulsar Apache Pulsar version 2.8.0 and prior versions; Apache Pulsar version 2.7.3 and prior versions; Apache Pulsar version 2.6.4 and prior versions.

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

CVE-2021-41040

In **Eclipse** Wakaama, ever since its inception until 2021-01-14, the CoAP parsing code does not properly sanitize network-received data.

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

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

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: unknown	Created: 2022-02-01	Updated: 2022-02-01

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: unknown	Created: 2022-02-01	Updated: 2022-02-01
---------	-----------------	---------------------	---------------------

CVE-2021-38560

Ivanti Service Manager 2021.1 allows reflected XSS via the appName parameter associated with ConfigDB calls, such as in RelocateAttachments.aspx.

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

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.

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

CVE-2021-46663

MariaDB through 10.5.13 allows a ha_maria::extra application crash via certain SELECT statements.

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

CVE-2021-46665

MariaDB through 10.5.9 allows a sql_parse.cc application crash because of incorrect used_tables expectations.

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

CVE-2021-46664

MariaDB through 10.5.9 allows an application crash in sub_select_postjoin_aggr for a NULL value of aggr.

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

Service (DoS) via a crafted PDF file.			
UNRATED	Vector: unknown	Created: 2022-02-01	Updated: 2022-02-01

CVE-2022-23603

iTunesRPC-Remastered is a **discord** rich presence application for use with iTunes & **Apple Music**. In code before commit 24f43aa user input is not properly sanitized and code injection is possible. Users are advised to upgrade as soon as is possible. There are no known workarounds for this issue.

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

CVE-2022-23596

Junrar is an open source **java** RAR archive library. In affected versions A carefully crafted RAR archive can trigger an infinite loop while extracting said archive. The impact depends solely on how the application uses the library, and whether files can be provided by malignant users. The problem is patched in 7.4.1. There are no known workarounds and users are advised to upgrade as soon as possible.

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

CVE-2021-46667

MariaDB before 10.6.5 has a sql_lex.cc integer overflow, leading to an application crash.

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

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.

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

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).

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

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.

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

CVE-2022-23602

Nimforum is a lightweight alternative to **Discourse** written in Nim. In versions prior to 2.2.0 any forum user can create a

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.

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

new thread/post with an include referencing a file local to the host operating system. Nimforum will render the file if able. This can also be done silently by using NimForum's post "preview" **endpoint**. Even if NimForum is running as a non-critical user, the forum.json secrets can be stolen. Version 2.2.0 of NimForum includes patches for this vulnerability. Users are advised to upgrade as soon as is possible. There are no known workarounds for this issue.

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

CVE-2022-0419

NULL Pointer Dereference in NPM **radare2.js** prior to 6.0.0.

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

CVE-2022-0401

Path Traversal in NPM w-zip prior to 1.0.12.

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

CVE-2016-3735

Piwigo is image **gallery** software written in PHP. When a criteria is not met on a host, piwigo defaults to using mt_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.

UNRATED	Vector: unkown	Created: 2022-01-28	Updated: 2022-02-01
---------	-------------------	------------------------	------------------------

CVE-2021-45416

Reflected Cross-site scripting (XSS) vulnerability in **RosarioSIS** 8.2.1 allows attackers to inject arbitrary HTML via the search_term parameter in the modules/Scheduling/Courses.php script.

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

CVE-2021-43509

SQL Injection vulnerability exists in **Sourcecodester** Simple Client Management System 1.0 via the id parameter in view-service.php.

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

CVE-2021-43510

SQL Injection vulnerability exists in **Sourcecodester** Simple Client Management System 1.0 via the username field in login.php.

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

CVE-2022-0408

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

UNRATED	Vector: unkown	Created: 2022-01-30	Updated: 2022-02-01
---------	-------------------	------------------------	------------------------

CVE-2022-23601

Symfony is a PHP **framework** for web and console applications and a set of reusable PHP components. The Symfony form component provides a CSRF protection mechanism by using a random token injected in the form and using the session to store and control the token submitted by the user. When using the FrameworkBundle, this protection can be enabled or disabled with the configuration. If the configuration is not specified, by default, the mechanism is enabled as long as the session is enabled. In a recent change in the way the configuration is loaded, the default behavior has been dropped and, as a result, the CSRF protection is not enabled in form when not explicitly enabled, which makes the application sensible to CSRF attacks. This issue has been resolved in the patch versions listed and users are advised to update. There are no known workarounds for this issue.

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

CVE-2021-24937

The Asset CleanUp: Page Speed **Booster WordPress** plugin before 1.3.8.5 does not

CVE-2021-24983

The Asset CleanUp: Page Speed **Booster WordPress** plugin before 1.3.8.5 does not sanitise and escape POSTed parameters

escape the wpacu_selected_sub tab area parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting issue

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

sent to the wpassetcleanup_fetch_active_plugins_icons AJAX **action** (available to admin users), leading to a Reflected Cross-Site Scripting issue

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

CVE-2021-24814

The check_privacy_settings AJAX **action** of the **WordPress** GDPR WordPress plugin before 1.9.26, available to both unauthenticated and authenticated users, responds with **JSON** data without an "application/json" content-type. Since an HTML payload isn't properly escaped, it may be interpreted by a web browser led to this **endpoint**. Javascript code may be executed on a victim's browser. If the victim is an administrator with a valid session cookie, full control of the WordPress instance may be taken (AJAX calls and **iframe** manipulation are possible because the vulnerable endpoint is on the same domain as the admin panel - there is no same-origin restriction).

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

CVE-2022-0220

The check_privacy_settings AJAX **action** of the **WordPress** GDPR WordPress plugin before 1.9.27, available to both unauthenticated and authenticated users, responds with **JSON** data without an "application/json" content-type. Since an HTML payload isn't properly escaped, it may be interpreted by a web browser led to this **endpoint**. Javascript code may be executed on a victim's browser. Due to v1.9.26 adding a CSRF check, the XSS is only exploitable against unauthenticated users (as they all share the same nonce)

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

CVE-2021-25063

The **Contact Form 7 Skins WordPress** plugin through 2.5.0 does not sanitise and escape the tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting

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

CVE-2021-24944

The Custom **Dashboard & Login Page WordPress** plugin before 7.0 does not sanitise some of its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.

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

CVE-2021-24775

The Document Embedder **WordPress** plugin before 1.7.5 contains a REST endpoint, which could allow unauthenticated users to enumerate the title of arbitrary private and draft posts.

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

CVE-2021-24868

The Document Embedder **WordPress** plugin before 1.7.9 contains a AJAX **action** endpoint, which could allow any authenticated user, such as subscriber to enumerate the title of arbitrary private and draft posts.

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

CVE-2021-24926

The Domain Check **WordPress** plugin before 1.0.17 does not sanitise and escape the domain parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting issue

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

CVE-2021-24761

The **Error Log Viewer WordPress** plugin through 1.1.1 does not perform nonce check when deleting a log file and does not have path traversal prevention, which could allow attackers to make a logged in admin delete arbitrary text files on the web server.

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

CVE-2022-0320

The Essential Addons for **Elementor WordPress** plugin before 5.0.5 does not validate and sanitise some template data before it them in include statements, which could allow unauthenticated attackers to perform Local File Inclusion attack and read arbitrary files on the server, this could also lead to RCE via user uploaded files or other LFI to RCE techniques.

CVE-2021-25097

The LabTools **WordPress** plugin through 1.0 does not have proper authorisation and CSRF check in place when deleting publications, allowing any authenticated users, such as subscriber to delete arbitrary publication

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

	<div>UNRATED</div> <div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div>		<div></div> <div>0101</div>
CVE-2021-24707	<div>The Learning Courses WordPress plugin before 5.0 does not sanitise and escape the Email PDT identity token settings, which could allow high privilege users to perform cross-Site Scripting attacks even when the <code>unfiltered_html</code> capability is disallowed</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>	CVE-2021-25093	<div>The Link Library WordPress plugin before 7.2.8 does not have authorisation in place when deleting links, allowing unauthenticated users to delete arbitrary links via a crafted request</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>
CVE-2021-25092	<div>The Link Library WordPress plugin before 7.2.8 does not have CSRF check when resetting library settings, allowing attackers to make a logged in admin reset arbitrary settings via a CSRF attack</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>	CVE-2021-25091	<div>The Link Library WordPress plugin before 7.2.9 does not sanitise and escape the <code>settingscopy</code> parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>
CVE-2021-24975	<div>The NextScripts: Social Networks Auto-Poster WordPress plugin before 4.3.24 does not sanitise and escape logged requests before outputting them in the related admin dashboard, leading to an Unauthenticated Stored Cross-Site Scripting issue</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>	CVE-2021-25072	<div>The NextScripts: Social Networks Auto-Poster WordPress plugin before 4.3.25 does not have CSRF check in place when deleting items, allowing attacker to make a logged in admin delete arbitrary posts via a CSRF attack</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>
CVE-2021-24900	<div>The Ninja Tables WordPress plugin before 4.1.8 does not sanitise and escape some of its table fields, which could allow high privilege users to perform Cross-Site Scripting attacks even when the <code>unfiltered_html</code> capability is disallowed</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>	CVE-2021-24763	<div>The Perfect Survey WordPress plugin before 1.5.2 does not have proper authorisation nor CSRF checks in the <code>save_global_setting</code> AJAX action, allowing unauthenticated users to edit surveys and modify settings. Given the lack of sanitisation and escaping in the settings, this could also lead to a Stored Cross-Site Scripting issue which will be executed in the context of a user viewing any survey</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>
CVE-2021-24764	<div>The Perfect Survey WordPress plugin before 1.5.2 does not sanitise and escape multiple parameters (<code>id</code> and <code>filters[session_id]</code> of <code>single_statistics</code> page, <code>type</code> and <code>message</code> of <code>importexport</code> page) before outputting them back in <code>pages/attributes</code> in the admin dashboard, leading to Reflected Cross-Site Scripting issues</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>	CVE-2021-24762	<div>The Perfect Survey WordPress plugin before 1.5.2 does not validate and escape the <code>question_id</code> GET parameter before using it in a SQL statement in the <code>get_question</code> AJAX action, allowing unauthenticated users to perform SQL injection.</div> <div><div>UNRATED</div><div>Vector: Created: Updated: unkown 2022-02-01 2022-02-01</div></div>
CVE-2021-24765	<div>The Perfect Survey WordPress plugin through 1.5.2 does not validate and escape the X-Forwarded-For header value before outputting it in the statistic page when the Anonymize IP setting of a survey is turned off, leading to a Stored Cross-Site Scripting issue</div> <div><div></div><div>Vector: Created: Updated:</div></div>	CVE-2021-24648	<div>The RegistrationMagic WordPress plugin before 5.0.1.9 does not sanitise and escape the <code>rm_search_value</code> parameter before outputting back in an attribute, leading to a Reflected Cross-Site Scripting</div> <div><div>UNRATED</div><div>Vector: Created: Updated: 2022-02-2022-02-</div></div>

UNRATED	unkown	2022-02-01	2022-02-01
---------	--------	------------	------------

	unkown	01	01
--	--------	----	----

CVE-2021-24686

The SVG Support **WordPress** plugin before 2.3.20 does not escape the "CSS Class to target" setting before outputting it in an attribute, which could allow high privilege users to perform Cross-Site Scripting attacks even when the `unfiltered_html` capability is disallowed.

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

CVE-2021-25089

The **UpdraftPlus WordPress Backup** Plugin WordPress plugin before 1.16.69 does not sanitise and escape the `updraft_restore` parameter before outputting it back in the Restore page, leading to a Reflected Cross-Site Scripting

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

CVE-2021-24934

The **Visual CSS Style Editor WordPress** plugin before 7.5.4 does not sanitise and escape the `wyp_page_type` parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting issue

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

CVE-2021-24919

The **Wicked Folders WordPress** plugin before 2.8.10 does not sanitise and escape the `folder_id` parameter before using it in a SQL statement in the `wicked_folders_save_sort_order` AJAX action, available to any authenticated user. leading to an SQL injection

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

CVE-2021-25085

The WOOF **WordPress** plugin before 1.2.6.3 does not sanitise and escape the `woof_redraw_elements` before outputting back in an admin page, leading to a Reflected Cross-Site Scripting

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

CVE-2022-23607

`treq` is an **HTTP library** inspired by requests but written on top of Twisted's Agents. `Treq`'s request methods (``treq.get``, ``treq.post``, etc.) and ``treq.client.HTTPClient`` constructor accept cookies as a dictionary. Such cookies are not bound to a single domain, and are therefore sent to **every** domain ("supercookies"). This can potentially cause sensitive information to leak upon an HTTP redirect to a different domain., e.g. should ``https://example.com`` redirect to ``http://cloudstorageprovider.com`` the latter will receive the cookie ``session``. `Treq 2021.1.0` and later **bind** cookies given to request methods (``treq.request``, ``treq.get``, ``HTTPClient.request``, ``HTTPClient.get``, etc.) to the **origin** of the **url** parameter. Users are advised to upgrade. For users unable to upgrade Instead of passing a dictionary as the **cookies** argument, pass a ``http.cookiejar.CookieJar`` instance with properly domain- and scheme-scoped cookies in it.

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

CVE-2021-44746

UNIVERGE DT 820 V3.2.7.0 and prior, UNIVERGE DT 830 V5.2.7.0 and prior, UNIVERGE DT 930 V2.4.0.0 and prior, **IP Phone** Manager V8.9.1 and prior, Data Maintenance Tool for DT900 Series V5.3.0.0 and prior, Data Maintenance Tool for DT800 Series V4.2.0.0 and prior allows a remote attacker who can access to the internal network, the configuration information may be obtained.

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

CVE-2022-0413

Use After Free in **GitHub** repository vim/vim prior to 8.2.

UNRATED	Vector: unkown	Created: 2022-01-30	Updated: 2022-02-01
---------	----------------	---------------------	---------------------

CVE-2021-43859

XStream is an open source **java** library to serialize objects to XML and back again. Versions prior to 1.4.19 may allow a remote attacker to allocate 100% CPU

time on the target system depending on CPU type or parallel execution of such a payload resulting in a denial of service only by manipulating the processed input stream. XStream 1.4.19 monitors and accumulates the time it takes to add elements to collections and throws an exception if a set threshold is exceeded. Users are advised to upgrade as soon as possible. Users unable to upgrade may set the NO_REFERENCE mode to prevent recursion. See GHSA-rmr5-cpv2-vgjf for further details on a workaround if an upgrade is not possible.

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

Source: *Hybrid Analysis*

Top malicious files

100% Threat score	Neton_Hybrid . exe	100% Threat score	invoice . pdf
100% Threat score	BlueStacksInstaller_5 . 5 . 101 . 1002_native_2d8f81038b36c696ac68fc6262df04bc_0 . exe	100% Threat score	details-83 . xls
100% Threat score	ChleebekClicker . exe	100% Threat score	CNB Payment Advice . xls
100% Threat score	ARCHIVO_0102 . xls	100% Threat score	BS_0102 . xls
100% Threat score	DOCUMENTO_0102 . xls	100% Threat score	Lista_37999 . xls
100% Threat score	kahuasetup . exe	100% Threat score	3_2 . exe
100% Threat score	N . dll	100% Threat score	Setup Cracked . exe
100% Threat score	Main-Pass--1234--setup . exe	100% Threat score	s 4 . xls
100% Threat score	s 4 . xls	100% Threat score	SmartLF MFP USB driver-Setup . exe
93% Threat score	MrY2fm . dll	92% Threat score	DGmXq . dll
92% Threat score	8mol9mVlBEsfca . dll	92% Threat score	2M9adan . dll
92% Threat score	6nLVRnASx . dll	91% Threat score	9kyef3NA . dll
91% Threat score	0HRimfr6WDCJpeW0 . dll	91% Threat score	2pJV5qU0 . dll
89% Threat score	Credit Invoice 934 . html	86% Threat score	GKM602R_Driver_v . 1 . 0 . exe
85%	googlechromestandaloneenterprise64_97 . 0 . 4692 .		

Threat score	99 . msi	85% Threat score	RWEnhancerPRO_1 . 03_Install . exe
80% Threat score	Firefox Setup 96 . 0 . 3 . msi	79% Threat score	Investing . docx

Source: *Hybrid Analysis*

Top malicious URL

100% Threat score	https://waltrack . net/saving-tips/waltrack-the-camelcamelcamel-for-walmart-com	100% Threat score	https://zombearwrites . com/
74% Threat score	http://spiritualgraphicdesign . fr/	74% Threat score	http://www . szechuanrestaurantsb . com/menu/Chinese_Full_Menu . pdf
72% Threat score	http://wildfarmalliance . org/		







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		#6 Michael Persaud

business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

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 Viet Nam



#6 United States of America



#7 Algeria



#8 Brazil



#9 Pakistan



#10 Iran (Islamic Republic of)

Source: [SpamHaus](#)

Top phishing countries



#1 United States



#2 Germany



#3 Netherlands



#4 Russia



#5 Singapore



#6 France



#7 India



#8 Turkey



#9 Chile



#10 Hong Kong