Security Rabbits

Your Security Rabbits report for February 22, 2022

Hot topics

Patch your Ubuntu

A vulnerability on "snap", a packaging software, has been discovered. It allows under certain conditions to gain root access. Around 40 million Ubuntu servers are impacted. Time to patch. The patches are already available.

```
sudo apt-get update
sudo apt-get upgrade
```

--
JL Dupont

News

Security Affairs

A cyber attack heavily impacted operations of Expeditors International

American worldwide logistics and freight forwarding company Expeditors International shuts down global operations after cyber attack American logistics and freight forwarding company Expeditors International was hit by a cyberattack over the weekend that paralyzed most of its operations worldwide. Expeditors company has over 18,000 employees worldwide and has annual gross revenue of around $10 billion. The company discovered the [...] The post A cyber attack heavily impacted operations of Expeditors International appeared first on Security Affairs.

Cyware News - Latest Cyber News

A Record Number of Phishing Attacks Leverage Linkedin

With an intention to steal personal details and cause further damages, spammers and phishers are duping working professionals with a variety of job lures that are distributed via email, SMS, or instant message.

Cyware News - Latest Cyber News

Attackers Target Top UK Bank With Phishing Campaigns

Monzo, one of the UK's most popular online banking platforms, warned users against an ongoing phishing campaign that can acquire their personal data and eventually, let hackers take over their bank accounts. The phishing process starts with a SMSdisplaying Monzo as the sender's name. Users need to remember that the platform does not use SMS for notification. They are recommended to stay cautious when receiving SMS from unknown sources or looking suspicious.

The Hacker

Chinese Hackers Target Taiwan's Financial Trading Sector with Supply Chain Attack

An advanced persistent threat (APT) group operating with objectives aligned with the Chinese

The Hacker News

A Free Solution to Protect Your Business from 6 Biggest Cyber Threats in 2022

For the last few years, the cybersecurity threat landscape has gotten progressively more complex and dangerous. The online world is now rife with data thieves, extortionists, and even state actors looking to exploit vulnerabilities in businesses' digital defenses. And unfortunately -- the bad guys have the upper hand at the moment. Part of the reason for that is the fallout from the rapid

ZDNet | security RSS

Almost 100,000 new mobile banking Trojan strains detected in 2021

Mobile malware used to be relatively rare. Now, the focus has pivoted from PCs to our handsets.

Cyware News - Latest Cyber News

China-linked APT10 Group Targeted Taiwan's Financial Sector in Months-long Attack Campaign

The attacks are believed to have started at the end of November 2021 and were still taking place this month, according to a report shared with The Record today by Taiwanese security firm CyCraft.

News

government has been linked to an organized supply chain attack on Taiwan's financial sector. The attacks are said to have first commenced at the end of November 2021, with the intrusions attributed to a threat actor tracked as APT10, also known as Stone Panda, the MenuPass group, and Bronze Riverside,

Cyware News - Latest Cyber News

Coinbase Pays $250K for 'Market-Nuking' Security Flaw

The root cause of the flaw was a missing logic validation check in a Retail Brokerage API endpoint, which allowed a user to submit trades to a specific order book using a mismatched source account.

Naked Security

French speakers blasted by sextortion scams with no text or links

You'd spot this one a mile away... but what about your friends or family?

Security Affairs

How SMS PVA services could undermine SMS-based verification

Crooks abuse some SMS PVA services that allow their customers to create disposable user accounts to conduct malicious activities. While investigating SMS PVA services (phone-verified account services), Trend Micro researchers discovered a rogue platform using a botnet of thousands of Android devices used to carry out malicious activities. SMS PVA services provide alternative mobile numbers [...] The post How SMS PVA services could undermine SMS-based verification appeared first on Security Affairs.

Cyware News - Latest Cyber News

Introducing Ghostbuster - AWS security tool protects against dangling elastic IP takeovers

Cybercriminals can identify vulnerable subdomains by continually claiming dangling elastic IPs until they find an IP associated with the subdomain of a targeted organization.

Cyware News - Latest Cyber News

Is Conti Behind the TrickBot Operation?

In new findings, the operators of the TrickBot trojan appear to have collaborated with the creators of the Conti ransomware. The reason behind this development could be the multiple takedown attempts on the TrickBot infrastructure. However, as per claims, the bot is dead; and moving forward they will use BazarBackdoor as a primary tool for initial access rather than TrickBot.

Cyware News -

Mobile malware evolution 2021

In 2021, Kaspersky researchers observed a downtrend in the number of attacks on mobile users. But attacks are becoming more sophisticated in terms of both malware functionality and vectors.

ZDNet | security RSS

CISA publishes guide with free cybersecurity tools, resources for incident response

The resources can provide a foundation for dealing with the aftermath of cyberattacks.

Cyware News - Latest Cyber News

Cracking the Code - Researchers Decrypt Hive Ransomware

Researchers identified a bug in the encryption algorithm of Hive ransomware, allowing white hat researchers to decrypt data without the need for any private key. Researchers could weaponize the flaw to recover 92-98% of the master key used during encryption. The method can now be effectively used to limit the damage caused by Hive ransomware.

The Hacker News

Hackers Backdoor Unpatched Microsoft SQL Database Servers with Cobalt Strike

Vulnerable internet-facing Microsoft SQL (MS SQL) Servers are being targeted by threat actors as part of a new campaign to deploy the Cobalt Strike adversary simulation tool on compromised hosts. "Attacks that target MS SQL servers include attacks to the environment where its vulnerability has not been patched, brute forcing, and dictionary attack against poorly managed servers," South Korean

WeLiveSecurity

Integer overflow: How does it occur and how can it be prevented?

Make no mistake, counting on a computer is not as easy as it may seem. Here's what happens when a number gets "too big". The post Integer overflow: How does it occur and how can it be prevented? appeared first on WeLiveSecurity

The Hacker News

Iranian State Broadcaster IRIB Hit by Destructive Wiper Malware

An investigation into the cyberattack targeting Iranian national media corporation, Islamic Republic of Iran Broadcasting (IRIB), in late January 2022 revealed in the deployment of a wiper malware and other custom implants, as the country's national infrastructure continues to face a wave of attacks aimed at inflicting serious damage. "This indicates that the attackers' aim was also to disrupt

Cyware News - Latest Cyber News

Latest Mac Coinminer Utilizes Open-Source Binaries and the I2P Network

The malicious actor can have a coinminer masquerade itself as a legitimate app, trick susceptible users into running it on their systems, and just wait for the profits to roll in.

The Hacker News

New Android Banking Trojan Spreading via Google Play Store Targets Europeans

A new Android banking trojan with over 50,000 installations has been observed distributed via the official Google Play Store with the goal of targeting 56 European banks and carrying out harvesting sensitive information from compromised devices. Dubbed Xenomorph by Dutch security firm

Latest Cyber News

Threatpost

NFT Investors Lose $1.7M in OpenSea Phishing Attack

Attackers took advantage of a smart-contract migration to swindle 17 users.

Cyware News - Latest Cyber News

Radware buys Israeli cybersecurity co SecurityDAM

Radware said that the $42.5 million acquisition of cloud security firm SecurityDAM is part of its strategic initiative to accelerate the growth of its cloud security service business.

Cyware News - Latest Cyber News

TitanHQ Announces Acquisition of Cyber Risk Aware

The acquisition will further bolster TitanHQ's already extensive security offering. Cyber Risk Aware delivers cyber security awareness training to staff in response to actual staff network behavior.

IT Security Guru

UK companies Omniscope and Searchlight Security team up to provide next-level threat intelligence

Two UK cybersecurity companies Searchlight Security, the provider of specialist deep and dark web monitoring products, and Omniscope, the digital threat intelligence and investigations business, have announced a partnership that brings next-level threat intelligence to enterprise customers and law enforcement agencies alike. The solution combines Omniscope's Smarti3 Intelligence platform for open-source threat intelligence of the […] The post UK companies Omniscope and Searchlight Security team up to provide next-level threat intelligence appeared first on IT Security Guru.

Cyware News - Latest Cyber News

Xenomorph Android Banking Trojan Spreads via Google Play Store to Target European Users

The trojan, with over 50,000 installations, has been distributed via the Google Play Store with the goal of targeting 56 European banks to harvest sensitive information from compromised devices.

ThreatFabric, the in-development malware is said to share overlaps with another banking trojan tracked under the

ZDNet | security RSS

NIST proposes model to assess cybersecurity investment strategies in network security

The larger the network, the larger the attack surface. Computational models may pinpoint the best places for investment.

ZDNet | security RSS

Scam artists swindle NFTs worth 'millions' in OpenSea phishing attack

The NFT platform is "working around the clock" to investigate.

Cyware News - Latest Cyber News

TunnelVision APT Group Exploits Log4Shell

SentinelOne allegedly stumbled across an Iranian threat actor, dubbed TunnelVision, exploiting the Log4j vulnerability on unpatched VMware Horizon servers with ransomware. The group exploited multiple one-day flaws, such as FortiOS (CVE-2018-13379) and Exchange (ProxyShell). The TTPs of TunnelVision overlap with Iran-linked nation-state actor - APT35.

Security Affairs

Xenomorph Android banking trojan distributed via Google Play Store

Xenomorph Android trojan has been observed distributed via the official Google Play Store targeting 56 European banks. Researchers from ThreatFabric have spotted a new Android banking trojan, dubbed Xenomorph, distributed via the official Google Play Store that has over 50,000 installations. The banking Trojan was used to target 56 European banks and steal sensitive information from […] The post Xenomorph Android banking trojan distributed via Google Play Store appeared first on Security Affairs.

Twitter

Official ATLUS West

In a war between Devil Summoners, it's up to Ringo and her team to decrypt destiny and save the world from apocalypse! Soul Hackers 2 releases August 26, 2022 for PlayStation 5, PlayStation 4, Xbox Series X|S, and Steam!

Klobrille

Atlus has finally acknowledged Xbox as a gaming platform. Soul Hackers 2 has just been announced for Xbox Series X|S and Xbox One, along with other platforms. Trailer:

Wario64

Soul Hackers 2 coming to PS4/PS5/XBO/XS/Steam/Win10/Win11 on August 26th

Why is no one talking about Soul Hackers 2 using

Official ATLUS West

Soul Hackers 2 will include English and Japanese voiceover options, with subtitles available in English, French, Italian, German, and Spanish!

Wario64

Shin Megami Tensei: Devil Summoner: Soul Hackers (3DS) available on US eShop for $19.99

LeGate

Trump announces Truth Social is down due to dumb as a rock developers and communist hackers[...] says site will be back online in 2 weeks

Soul Hackers

Jon Cartwright

enemy designs DIRECTLY from Persona????

SEGA Europe

In a war between devil summoners, its up to Ringo and her team to decrypt destiny and save the world from apocalypse! Soul Hackers 2 releases August 26, 2022 for Xbox Series X|S, PlayStation 5, PlayStation 4, and Steam!

Sahara Reporters

No Document Shows Buharis Minister, Pantami Is Cyber Security Expert Despite Appointment As Professor By Nigerian University, FUTO Report | Sahara Reporters

Casey Mongillo

Jon Cartwright

Xbox is getting Soul Hackers 2??

Ultima | #

Soul Hackers 2 looks like a lot of fun and I am excited its coming out so soon with a global release date, but its gonna be mad funny if it blows whatever Persona related announcement they were supposed to put out this month out of the water.

Source: NIST

NIST CVE: Critical

Nothing today

Source: NIST

NIST CVE: High

Nothing today

Source: NIST

NIST CVE: Medium

CVE-2022-23053

Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the "Condition Widget" element, that allows the injection of malicious JavaScript into the 'URL' field. This issue affects: **nasa** openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.

MEDIUM	Vector: network	Created: 2022-02-20	Updated: 2022-02-22

CVE-2022-22126

Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the "Web Page" element, that allows the injection of malicious JavaScript into the 'URL' field. This issue affects: **nasa** openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.

MEDIUM	Vector: network	Created: 2022-02-20	Updated: 2022-02-22

CVE-2022-23054

Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the "Summary Widget" element, that allows the injection of malicious JavaScript into the 'URL' field. This issue affects: **nasa** openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.

MEDIUM	Vector: network	Created: 2022-02-20	Updated: 2022-02-22

Source: NIST

NIST CVE: Low

Nothing today

Source: NIST

NIST CVE: Unrated

CVE-2021-27753

"Sametime **Android** PathTraversal Vulnerability"

Created: Updated:

CVE-2021-27755

"Sametime **Android** potential path traversal vulnerability when using File class"

UNRATED Vector: unkown 2022-02-21 2022-02-22

CVE-2022-25358

A ..%2F path traversal vulnerability exists in the path handler of awful-salmonella-tar before 0.0.4. Attackers can only list directories (not read files). This occurs because the safe-path? Scheme predicate is not used for directories.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-25132

A command injection vulnerability in the function meshSlaveDlfw of **TOTOLINK** Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25135

A command injection vulnerability in the function recv_mesh_info_sync of **TOTOLINK** Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25137

A command injection vulnerability in the function recvSlaveUpgstatus of **TOTOLINK** Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25130

A command injection vulnerability in the function updateWifiInfo of **TOTOLINK** Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2021-44571

A heap overflow vulnerability exisfts in **openSUSE libsolv** through 13 Dec 2020 in the prefer_suggested function at src/policy.c: line 442.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44574

A heap-overflow vulnerability exists in **openSUSE libsolv** through 13 Dec 2020 in the resolve_jobrules function at

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-25133

A command injection vulnerability in the function isAssocPriDevice of **TOTOLINK** Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25136

A command injection vulnerability in the function meshSlaveUpdate of **TOTOLINK** Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25131

A command injection vulnerability in the function recvSlaveCloudCheckStatus of **TOTOLINK** Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25134

A command injection vulnerability in the function setUpgradeFW of **TOTOLINK** Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted **MQTT** packet.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-0563

A flaw was found in the **util-linux** chfn and chsh utilities when compiled with **Readline** support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44569

A heap-buffer **openSUSE libsolv** through 13 Dec 2020 exists in the solver_solve function at src/solver.c: line 3445.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-40841

A Path Traversal vulnerability for a log file in LiveConfig 2.12.2 allows authenticated src/solver.c at line 1599.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-40840

A Stored XSS issue exists in the admin/users user administration form in LiveConfig 2.12.2.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-0564

A vulnerability in **Qlik** Sense Enterprise on **Windows** could allow an remote attacker to enumerate domain user accounts. An attacker could exploit this vulnerability by sending authenticated requests to an affected system. A successful exploit could allow the attacker to compare the response time that are returned by the affected system to **determine** which accounts are valid user accounts. Affected systems are only vulnerable if they have **LDAP** configured.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-46036

An arbitrary file upload vulnerability in the component /ms/file/uploadTemplate.do of **MCMS** v5.2.4 allows attackers to execute arbitrary code.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-45082

An issue was discovered in **Cobbler** before 3.3.1. In the templar.py file, the function check_for_invalid_imports can allow Cheetah code to import **Python** modules via the "#from MODULE import" substring. (Only lines beginning with #import are blocked.)

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25375

An issue was discovered in drivers/usb/gadget/function/rndis.c in the **Linux** kernel before 5.16.10. The RNDIS USB gadget lacks validation of the size of the RNDIS_MSG_SET command. Attackers can obtain sensitive information from kernel memory.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2022-24979

An issue was discovered in the Varnishcache extension before 2.0.1 for **TYPO3**. The **Edge** Site Includes (ESI) content element renderer component does

attackers to read files on the underlying server.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-27796

A vulnerability in **Brocade Fabric OS** versions before **Brocade Fabric OS** v8.0.1b, v7.4.1d could allow an authenticated attacker within the restricted shell environment (rbash) as either the "user" or "factory" account, to read the contents of any file on the filesystem utilizing one of a few available binaries.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44141

All versions of **Samba** prior to 4.15.5 are vulnerable to a malicious client using a server symlink to **determine** if a file or directory exists in an area of the server file system not exported under the share definition. SMB1 with **unix** extensions has to be enabled in order for this attack to succeed.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-45083

An issue was discovered in **Cobbler** before 3.3.1. Files in /etc/cobbler are world readable. Two of those files contain some sensitive information that can be exposed to a local user who has non-privileged access to the server. The users.digest file contains the sha2-512 digest of users in a Cobbler local installation. In the case of an easy-to-guess password, it's trivial to obtain the plaintext string. The settings.yaml file contains secrets such as the hashed default password.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2021-45081

An issue was discovered in **Cobbler** through 3.3.1. Routines in several files use the HTTP protocol instead of the more secure HTTPS.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2022-24980

An issue was discovered in the **Kitodo**.Presentation (aka dif) extension before 2.3.2, 3.x before 3.2.3, and 3.3.x before 3.3.4 for **TYPO3**. A missing access check in an eID script allows an unauthenticated user to submit arbitrary URLs to this component. This results in SSRF, allowing attackers to view the content of any file or webpage the webserver has access to.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

not include an access check. This allows an unauthenticated user to render various content elements, resulting in insecure direct object reference (IDOR), with the potential of exposing internal content elements.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-0686

Authorization Bypass Through User-Controlled Key in NPM **url-parse** prior to 1.5.8.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2021-44302

BaiCloud-cms v2.5.7 was discovered to contain multiple SQL injection vulnerabilities via the tongji and baidu_map parameters in /user/ztconfig.php.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-0688

Business Logic Errors in Packagist microweber/microweber prior to 1.2.11.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2022-23649

Cosign provides container signing, verification, and storage in an OCI **registry** for the sigstore project. Prior to version 1.5.2, Cosign can be manipulated to claim that an entry for a signature exists in the Rekor transparency log even if it doesn't. This requires the attacker to have pull and push permissions for the signature in OCI. This can happen with both standard signing with a keypair and "keyless signing" with Fulcio. If an attacker has access to the signature in OCI, they can manipulate cosign into believing the entry was stored in Rekor even though it wasn't. The vulnerability has been patched in v1.5.2 of Cosign. The `signature` in the `signedEntryTimestamp` provided by Rekor is now compared to the `signature` that is being verified. If these don't match, then an error is returned. If a valid bundle is copied to a different signature, verification should fail. Cosign output now only informs the user that certificates were verified if a certificate was in fact verified. There is currently no known workaround.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-23983

Cross-Site Request Forgery (CSRF) vulnerability leading to plugin Settings Update discovered in WP Content Copy Protection & No Right Click **WordPress** plugin (versions <= 3.4.4).

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

CVE-2022-24553

An issue was found in Zfaka <= 1.4.5. The verification of the background file upload function check is not strict, resulting in remote command execution.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0691

Authorization Bypass Through User-Controlled Key in NPM **url-parse** prior to 1.5.9.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-27797

Brocade Fabric OS before **Brocade Fabric OS** v8.2.1c, v8.1.2h, and all versions of Brocade Fabric OS v8.0.x and v7.x contain documented hard-coded credentials, which could allow attackers to gain access to the system.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-24564

Checkmk <=2.0.0p19 contains a Cross Site Scripting (XSS) vulnerability. While creating or editing a user attribute, the Help Text is subject to HTML injection, which can be triggered for editing a user.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-25599

Cross-Site Request Forgery (CSRF) vulnerability leading to event deletion was discovered in **Spiffy** Calendar **WordPress** plugin (versions <= 4.9.0).

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0690

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

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

unkown 21 22

CVE-2022-0678

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

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-25365

Docker Desktop before 4.5.1 on **Windows** allows attackers to move arbitrary files. NOTE: this issue exists because of an incomplete fix for CVE-2022-23774.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-0676

Heap-based Buffer Overflow in **GitHub** repository radareorg/radare2 prior to 5.6.4.

UNRATED Vector: unkown Created: 2022-02-22 Updated: 2022-02-22

CVE-2022-23848

In Alluxio before 2.7.3, the logserver does not validate the input stream. NOTE: this is not the same as the CVE-2021-44228 **Log4j** vulnerability.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2022-0543

It was discovered, that redis, a persistent key-value database, due to a packaging issue, is prone to a (Debian-specific) Lua sandbox escape, which could result in remote code execution.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46037

MCMS v5.2.4 was discovered to contain an arbitrary file deletion vulnerability via the component /template/unzip.do.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46062

MCMS v5.2.5 was discovered to contain an arbitrary file deletion vulnerability via the component oldFileName.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-25366

Cryptomator through 1.6.5 allows DYLIB injection because, although it has the flag 0x1000 for Hardened Runtime, it has the com.apple.security.cs.disable-library-validation and com.apple.security.cs.allow-dyld-environment-variables entitlements. An attacker can exploit this by creating a malicious .dylib file that can be executed via the DYLD_INSERT_LIBRARIES environment variable.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2016-1239

duck before 0.10 did not properly handle loading of untrusted code from the current directory.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-22308

IBM Planning Analytics 2.0 is vulnerable to a Remote File Include (RFI) attack. User input could be passed into file include commands and the web application could be tricked into including remote files with malicious code. IBM X-Force ID: 216891.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-46700

In **libsixel** 1.8.6, sixel_encoder_output_without_macro (called from sixel_encoder_encode_frame in encoder.c) has a double free.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-0708

Mattermost 6.3.0 and earlier fails to **protect** email addresses of the **creator** of the team via one of the APIs, which allows authenticated team **members** to access this information resulting in sensitive & private information disclosure.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-46063

MCMS v5.2.5 was discovered to contain a Server Side Template Injection (SSTI) vulnerability via the Template Management module.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2017-0371

MediaWiki before 1.23.16, 1.24.x through 1.27.x before 1.27.2, and 1.28.x before 1.28.1 allows remote attackers to **discover** the IP addresses of Wiki visitors via a style="background-image: attr(title url);" attack within a DIV element that has an attacker-controlled URL in the title attribute.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-23650

Netmaker is a platform for creating and managing virtual overlay networks using

CVE-2021-46082

Moxa TN-5900 v3.1 series routers, MGate 5109 v2.2 series protocol gateways, and MGate 5101-PBM-MN v2.1 series protocol gateways were discovered to contain a memory leak which allows attackers to cause a Denial of Service (DoS) via crafted packets.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-0696

NULL Pointer Dereference in **GitHub** repository vim/vim prior to 8.2.4428.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-24867

Numerous **Plugins** and Themes from the AccessPress Themes (aka Access Keys) vendor are backdoored due to their website being compromised. Only plugins and themes downloaded via the vendor website are affected, and those hosted on **wordpress**.org are not. However, all of them were updated or removed to avoid any confusion

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-46110

Online Shopping Portal v3.1 was discovered to contain multiple time-based SQL injection vulnerabilities via the email and contactno parameters.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-0630

Out-of-bounds Read in Homebrew **mruby** prior to 3.2.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2021-29656

Pexip Infinity Connect before 1.8.0 mishandles TLS certificate validation. The allow list is not properly checked.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-45007

Plesk 18.0.37 is affected by a Cross Site Request Forgery (CSRF) vulnerability that allows an attacker to insert data on the user and admin panel.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2021-46701

PreMiD 2.2.0 allows unintended access via the **websocket** transport. An attacker can receive events from a socket and emit events to a socket, potentially interfering with a victim's "now playing" **status** on **Discord**.

Created: Updated:

WireGuard. Prior to versions 0.8.5, 0.9.4, and 010.0, there is a hard-coded cryptographic key in the code base which can be exploited to run admin commands on a remote server if the exploiter know the address and username of the admin. This effects the server (netmaker) component, and not clients. This has been patched in Netmaker v0.8.5, v0.9.4, and v0.10.0. There are currently no known workarounds.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-0632

NULL Pointer Dereference in Homebrew **mruby** prior to 3.2.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-24295

Okta Advanced Server Access Client for **Windows** prior to version 1.57.0 was found to be vulnerable to command injection via a specially crafted URL.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0692

Open Redirect on Rudloff/alltube in Packagist rudloff/alltube prior to 3.0.1.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-23228

Pexip Infinity before 27.0 has improper **WebRTC** input validation. An unauthenticated remote attacker can use excessive resources, temporarily causing denial of service.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-29655

Pexip Infinity Connect before 1.8.0 omits certain provisioning authenticity checks. Thus, untrusted code may execute.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-45008

Plesk CMS 18.0.37 is affected by an insecure permissions vulnerability that allows privilege Escalation from user to admin rights.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-25372

Pritunl Client through 1.2.3019.52 on **Windows** allows local privilege escalation, related to an ACL entry for **CREATOR** OWNER in platform_windows.go.

Vector: Created: Updated:

UNRATED Vector: unkown 2022-02-20 2022-02-22

CVE-2022-25256

SAS Web **Report Studio** 4.4 allows XSS. /SASWebReportStudio/logonAndRender.do has two parameters: saspfs_request_backlabel_list and saspfs_request_backurl_list. The **first** one affects the content of the button placed in the top left. The second affects the page to which the user is directed after pressing the button, e.g., a malicious web page. In addition, the second parameter executes JavaScript, which means XSS is possible by adding a javascript: URL.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2016-20013

sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of service (CPU consumption) because the algorithm's **runtime** is proportional to the **square** of the length of the password.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-23645

swtpm is a libtpms-based TPM emulator with socket, character device, and **Linux** CUSE interface. Versions prior to 0.5.3, 0.6.2, and 0.7.1 are vulnerable to out-of-bounds read. A specially crafted header of swtpm's state, where the blobheader's hdrsize indicator has an invalid value, may cause an out-of-bounds access when the byte array representing the state of the TPM is accessed. This will likely crash swtpm or prevent it from starting since the state cannot be understood. Users should upgrade to swtpm v0.5.3, v0.6.2, or v0.7.1 to receive a patch. There are currently no known workarounds.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-24921

The Advanced Database Cleaner **WordPress** plugin before 3.0.4 does not sanitise and escape $_GET keys and values before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0134

The **AnyComment WordPress** plugin before 0.2.18 does not have CSRF checks in the Import and Revert HyperComments features, allowing attackers to make logged in admin perform such actions via a CSRF

UNRATED unkown 2022-02-20 2022-02-22

CVE-2022-23984

Sensitive information disclosure discovered in **wpDiscuz WordPress** plugin (versions <= 7.3.11).

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-23642

Sourcegraph is a code search and navigation engine. Sourcegraph prior to version 3.37 is vulnerable to remote code execution in the `gitserver` service. The service acts as a git exec proxy, and fails to properly restrict calling `git config`. This allows an attacker to set the git `core.sshCommand` option, which sets git to use the specified command instead of ssh when they need to **connect** to a remote system. Exploitation of this vulnerability depends on how Sourcegraph is deployed. An attacker able to make HTTP requests to internal services like gitserver is able to exploit it. This issue is patched in Sourcegraph version 3.37. As a workaround, ensure that requests to gitserver are properly protected.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-0288

The Ad Inserter **WordPress** plugin before 2.7.10, Ad Inserter Pro WordPress plugin before 2.7.10 do not sanitise and escape the html_element_selection parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25101

The **Anti-Malware** Security and Brute-Force **Firewall WordPress** plugin before 4.20.94 does not sanitise and escape the POST data before outputting it back in attributes of an admin page, leading to a Reflected Cross-Site scripting. Due to the presence of specific parameter value, available to admin users, this can only be exploited by an admin against another admin user.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0279

The **AnyComment WordPress** plugin before 0.2.18 is affected by a race condition when liking/disliking a comment/reply, which could allow any authenticated user to quickly raise attack

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25058

The Buffer Button **WordPress** plugin through 1.0 was vulnerable to Authenticated Stored Cross Site Scripting (XSS) within the **Twitter** username to mention text field.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0199

The Coming soon and Maintenance mode **WordPress** plugin before 3.6.8 does not have CSRF check in its coming_soon_send_mail AJAX action, allowing attackers to make logged in admin to send arbitrary emails to all subscribed users via a CSRF attack

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25069

The **Download Manager WordPress** plugin before 3.2.34 does not sanitise and escape the package_ids parameter before using it in a SQL statement, leading to a SQL injection, which can also be exploited to cause a Reflected Cross-Site Scripting issue

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-4208

The ExportFeed **WordPress** plugin through 2.0.1.0 does not sanitise and escape the product_id POST parameter before using it in a SQL statement, leading to a SQL injection vulnerability exploitable by high privilege users

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25060

The Five **Star** Business Profile and **Schema WordPress** plugin before 2.1.7 does not have any authorisation and CSRF in its bpfwp_welcome_add_contact_page and bpfwp_welcome_set_contact_information AJAX action, allowing any authenticated users, such as subscribers, to call them. Furthermore, due to the lack of sanitisation, it also lead to Stored Cross-Site Scripting issues

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0252

The **GiveWP WordPress** plugin before 2.17.3 does not escape the json parameter before outputting it back in an attribute in the Import admin dashboard, leading to a Reflected Cross-Site Scripting

UNRATED Vector: Created: 2022-02- Updated:

their **rating** or lower the rating of other users

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0164

The Coming soon and Maintenance mode **WordPress** plugin before 3.6.8 does not have authorisation and CSRF checks in its coming_soon_send_mail AJAX action, allowing any authenticated users, with a role as low as subscriber to send arbitrary emails to all subscribed users

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0255

The Database **Backup** for **WordPress** plugin before 2.5.1 does not properly sanitise and escape the fragment parameter before using it in a SQL statement in the admin dashboard, leading to a SQL injection issue

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25075

The Duplicate Page or Post **WordPress** plugin before 1.5.1 does not have any authorisation and has a flawed CSRF check in the wpdevart_duplicate_post_parametrs_save_in_db AJAX action, allowing any authenticated users, such as subscriber to call it and change the plugin's settings, or perform such attack via CSRF. Furthermore, due to the lack of escaping, this could lead to Stored Cross-Site Scripting issues

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25055

The **FeedWordPress** plugin before 2022.0123 is affected by a Reflected Cross-Site Scripting (XSS) within the "visibility" parameter.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0313

The Float menu **WordPress** plugin before 4.3.1 does not have CSRF check in place when deleting menu, which could allow attackers to make a logged in admin delete them via a CSRF attack

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25100

The **GiveWP WordPress** plugin before 2.17.3 does not escape the s parameter before outputting it back in an attribute in the Donation **Forms** dashboard, leading to a Reflected Cross-Site Scripting

Vector: Created: Updated:

unkown 21 2022-02-22

CVE-2021-25099

The **GiveWP WordPress** plugin before 2.17.3 does not sanitise and escape the form_id parameter before outputting it back in the response of an unauthenticated request via the give_checkout_login AJAX action, leading to a Reflected Cross-Site Scripting

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-23702

The package object-extend from 0.0.0 are vulnerable to Prototype Pollution via object-extend.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-25082

The **Popup** Builder **WordPress** plugin before 4.0.7 does not validate and sanitise the sgpb_type parameter before using it in a require statement, leading to a Local File Inclusion issue. Furthermore, since the beginning of the string can be controlled, the issue can lead to RCE vulnerability via wrappers such as PHAR

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0211

The Shield Security **WordPress** plugin before 13.0.6 does not sanitise and escape admin notes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0234

The WOOCS **WordPress** plugin before 1.3.7.5 does not sanitise and escape the woocs_in_order_currency parameter of the woocs_get_products_price_html AJAX **action** (available to both unauthenticated and authenticated users) before outputting it back in the response, leading to a Reflected Cross-Site Scripting

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-25297

This affects the package drogonframework/drogon before 1.7.5. The unsafe handling of file names during upload using HttpFile::save() method may enable attackers to write files to arbitrary locations outside the designated target folder.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

UNRATED unkown 2022-02-21 2022-02-22

CVE-2022-0186

The Image Photo **Gallery** Final Tiles **Grid WordPress** plugin before 3.5.3 does not sanitise and escape the Description field when editing a gallery, allowing users with a role as low as contributor to perform Cross-Site Scripting attacks against other users having access to the gallery dashboard

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0228

The **Popup** Builder **WordPress** plugin before 4.0.7 does not validate and properly escape the orderby and order parameters before using them in a SQL statement in the admin dashboard, which could allow high privilege users to perform SQL injection

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44142

The **Samba** vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with **Apple** SMB clients and interoperability with a **Netatalk** 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-25057

The Translation **Exchange WordPress** plugin through 1.0.14 was vulnerable to Authenticated Stored Cross-Site Scripting (XSS) within the Project Key text field found in the plugin's settings.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-4115

There is a flaw in **polkit** which can allow an unprivileged user to cause polkit to crash, due to process file descriptor exhaustion. The highest threat from this vulnerability is to availability. NOTE: Polkit process outage duration is tied to the failing process being reaped and a new one being spawned

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-24051

This vulnerability allows local attackers to escalate privileges on affected installations of **MariaDB**. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16193.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24052

This vulnerability allows local attackers to escalate privileges on affected installations of **MariaDB**. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16190.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2022-24050

This vulnerability allows local attackers to escalate privileges on affected installations of **MariaDB**. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16207.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2022-24354

This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of **TP-Link** AC1750 prior to 1.1.4 Build 20211022 rel.59103(5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the **NetUSB.ko** module. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15835.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2022-24047

This vulnerability allows remote attackers to bypass authentication on affected installations of BMC Track-It! 20.21.01.102. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-14618.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46602

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80.

CVE-2022-24048

This vulnerability allows local attackers to escalate privileges on affected installations of **MariaDB**. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16191.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2022-24046

This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Sonos One Speaker prior to 3.4.1 (S2 systems) and 11.2.13 build 57923290 (S1 systems). Authentication is not required to exploit this vulnerability. The specific flaw exists within the anacapd daemon. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15828.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2022-24355

This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of **TP-Link TL-WR940N** 3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of file name extensions. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-13910.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46595

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15389.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46607

This vulnerability allows remote attackers to disclose sensitive information on affected

User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15396.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46615

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15409.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46589

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15383.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46649

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15535.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15401.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46616

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15410.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46637

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15509.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46650

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15536.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46651

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15537.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46594

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15388.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46620

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of FBX files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15414.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46600

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15394.

		Created:	Updated:

CVE-2021-46593

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15387.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46608

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15402.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46611

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15405.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46610

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15404.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

UNRATED Vector: unkown 2022-02-18 2022-02-22

CVE-2021-46596

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of OBJ files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15390.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46599

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15393.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46618

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PNG images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15412.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46623

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15453.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46628

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15458.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46629

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15459.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46642

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of

CVE-2021-46654

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the

the current process. Was ZDI-CAN-15514.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46624

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15454.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46632

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15462.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24368

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16115.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24060

This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante **DICOM** Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DCM files. Crafted data in a DCM file can trigger a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of

current process. Was ZDI-CAN-15540.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46630

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of FBX files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15460.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46570

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Bentley** View 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15364.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24370

This vulnerability allows remote attackers to disclose sensitive information on affected installations of **Foxit PDF Reader Foxit reader** 11.0.1.0719 **macOS**. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA **forms**. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14819.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24061

This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante **DICOM** Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DCM files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code the current process. Was ZDI-CAN-15099.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24055

This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante **DICOM** Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of GIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14972.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46586

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. Crafted data in a 3DS file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15380.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46592

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15386.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46605

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15399.

in the context of the current process. Was ZDI-CAN-15100.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46621

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of JT files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15415.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46587

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of 3DS files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15381.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46645

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. Crafted data in a BMP image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15531.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46606

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15400.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46647

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15533.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46635

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15507.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46644

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15530.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46648

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15534.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46636

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15508.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46639

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15511.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46646

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15532.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46638

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15510.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46575

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15369.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46622

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K image can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15416.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46584

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15378.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46603

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15397.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46562

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation**

CVE-2021-46613

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15407.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46583

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15377.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46614

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15408.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46582

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15376.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46563

This vulnerability allows remote attackers to execute arbitrary code on affected installations

CONNECT 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14987.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46590

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15384.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46564

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15023.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46569

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15031.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46574

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to

of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14990.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46591

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15385.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46568

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15030.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46572

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15366.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46576

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15368.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46581

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15375.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46566

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15027.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46565

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15024.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46598

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15392.

Created: Updated:

execute code in the context of the current process. Was ZDI-CAN-15370.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46634

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15464.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46577

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15371.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46585

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15379.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46567

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15028.

Vector: Created: Updated:

UNRATED	Vector: unkown	2022-02-18	2022-02-22

CVE-2021-46573

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15367.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46579

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15373.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46588

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15382.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46601

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15395.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

UNRATED	unkown	2022-02-18	2022-02-22

CVE-2021-46578

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15372.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46580

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15374.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46597

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15391.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46612

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. Crafted data in a PDF file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15406.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46619

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. Crafted data in a PDF file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15413.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46633

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15463.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46617

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TIF images. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15411.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46653

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15539.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46640

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a

CVE-2021-46609

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15403.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46604

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley MicroStation CONNECT** 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PNG images. Crafted data in a PNG image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15398.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46625

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of JT files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15455.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46641

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN file. Crafted data in a DNG file can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15513.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-46652

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15512.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46643

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15515.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46626

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K image can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15456.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46655

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15630.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46571

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.16.0.80. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this

required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DGN files. Crafted data in a DGN file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15538.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46627

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15457.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46656

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JT files. Crafted data in a JT file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15631.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2021-46631

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Bentley** View 10.15.0.75. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TIF images. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15461.

UNRATED	Vector: unkown	Created: 2022-02-18	Updated: 2022-02-22

CVE-2022-24365

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An vulnerability to execute code in the context of the current process. Was ZDI-CAN-15365.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24366

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15853.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24363

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15861.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24358

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. By performing actions in JavaScript, an attacker can trigger a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15703.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24360

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15744.

attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15852.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24367

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15877.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24357

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15743.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24364

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15851.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24359

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Doc objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15702.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24362

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15987.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24971

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15812.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24356

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader Foxit reader** 11.0.1.0719 **macOS**. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the OnMouseExit method. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14848.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24058

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante **DICOM** Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15095.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24369

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 images. Crafted data in a JP2 image can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-16087.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24361

This vulnerability allows remote attackers to execute arbitrary code on affected installations of **Foxit PDF Reader** 11.1.0.52543. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15811.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24059

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante **DICOM** Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DCM files. Crafted data in a DCM file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-15098.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24057

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante **DICOM** Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15077.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24056

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante **DICOM** Viewer Pro 11.8.7.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K files. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15076.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24063

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante **DICOM** Viewer Pro 13.2.0.21165. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15105.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24049

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sonos One Speaker prior to 3.4.1 (S2 systems) and 11.2.13 build 57923290 (S1 systems). Authentication is not required to exploit this vulnerability. The specific flaw exists within the ALAC audio **codec**. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15798.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-44577

Two heap-overflow vulnerabilities **exist** in **openSUSE libsolv** through 13 Dec 2020 **bugs** in the propagate function at src/solver.c: line 490 and 524.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44575

Two heap-overflow vulnerabilities exists in **openSUSE libsolv** through 13 Dec 2020 in the makeruledecisions function at src/solver.c: line 147 and 307.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44576

Two memory vulnerabilities exists in **openSUSE libsolv** through 13 Dec 2020 in the resolve_weak function at

CVE-2022-24064

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante **DICOM** Viewer Pro 11.8.8.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of J2K images. Crafted data in a J2K file can trigger a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15161.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2022-24062

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante **DICOM** Viewer Pro 13.2.0.21165. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15104.

UNRATED Vector: unkown Created: 2022-02-18 Updated: 2022-02-22

CVE-2021-44573

Two heap overflow vulnerabilities **exist** in oenSUSE **libsolv** through 13 Dec 2020 in the resolve_installed function at src/solver.c: line 1728 & 1766.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44568

Two heap-overflow vulnerabilities **exist** in openSUSE/libsolv libsolv through 13 Dec 2020 in the decisionmap variable via the resolve_dependencies function at src/solver.c (line 1940 & line 1995), which could cause a remote Denial of Service.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-44570

Two heap-overflow vulnerabilities exists in openSUSE/libsolv through 13 Dec 2020 in the **bugs** in the solver_get_recommendations funtion function at src/solver.c: line 4286 & line 4305 FOR_PROVIDES.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2021-26256

Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability discovered in **Survey** Maker src/solver.c: line 2222 and 2249.

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0409

Unrestricted Upload of File with Dangerous Type in Packagist showdoc/showdoc prior to 2.10.2.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-0685

Use of Out-of-range Pointer Offset in **GitHub** repository vim/vim prior to 8.2.4418.

UNRATED Vector: unkown Created: 2022-02-20 Updated: 2022-02-22

CVE-2022-23376

WikiDocs version 0.1.18 has multiple reflected XSS vulnerabilities on different pages.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

WordPress plugin (versions <= 2.0.6).

UNRATED Vector: unkown Created: 2022-02-21 Updated: 2022-02-22

CVE-2022-0689

Use multiple time the one-time coupon in Packagist microweber/microweber prior to 1.2.11.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

CVE-2022-23375

WikiDocs version 0.1.18 has an authenticated remote code execution vulnerability. An attacker can upload a malicious file using the image upload form through index.php.

UNRATED Vector: unkown Created: 2022-02-19 Updated: 2022-02-22

Source: Hybrid Analysis

Top malicious files

100% Threat score — Box-x86 (.) msi

100% Threat score — 466caacba5e5830132bf6db74ee2b6f202676705ab38e6b989d559a302eac75c (.) msi

100% Threat score — syswranalyzer (.) exe

100% Threat score — bss-scanne2r (.) exe

85% Threat score — Cyberduck-Installer-8 (.) 2 (.) 3 (.) 36880 (.) exe

100% Threat score — 4090850000 (.) exe

100% Threat score — xxx (.) exe

100% Threat score — 8888888 (.) png

85% Threat score — npp (.) 8 (.) 3 (.) 1 (.) Installer (.) x64 (.) exe

77% Threat score — easyEmission64 (.) msi

Source: Hybrid Analysis

Top malicious URL

100% Threat score — https://citylex (.) nl/?anatoliy (.) reinhardt%40mobileye (.) com

93% Threat score — http://112 (.) 248 (.) 111 (.) 196:33996/mozi (.) m

93% Threat score — http://219 (.) 138 (.) 189 (.) 123:39840/mozi (.) a

79% Threat score — https://clck (.) ru/bn7pW?wwfd

95% Threat score — http://59 (.) 94 (.) 130 (.) 248:54531/bin (.) sh

93% Threat score — http://112 (.) 232 (.) 66 (.) 38:55732/i

92% Threat score — http://www (.) btlawfirm (.) com/wp-content/plugins/si-contact-form/captcha-secureimage/securimage_stop (.) php

79% Threat score — https://clck (.) ru/bn6hS?w64d

77% Threat score	http://inter-fairs (.) space/
77% Threat score	http://bit (.) do/Forum21
77% Threat score	http://ipfonline (.) org/
74% Threat score	http://www (.) ndaatgal (.) mn/v1/js/owl (.) autoplay (.) js

Source: SpamHaus

Top spamming countries

#1 United States of America

#2 China

#3 Russian Federation

#4 Mexico

#5 Dominican Republic

#6 Saudi Arabia

#7 India

#8 Japan

#9 Brazil

#10 Korea, Republic of

Source: SpamHaus

Top spammers

#1 **Canadian Pharmacy**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese & Russian web hosting.

#2 **PredictLabs / Sphere Digital**
This operation uses dozens of "hosting" companies as fronts to lease IP addresses which are then used to send spam. Based in Chicago, Illinois and Tangier, Morocco.

#3 **Hosting Response / Michael Boehm**
Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IP addresses and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names. Owner or manager of these companies seems to be Michael Boehm and Associates.

#4 **Mint Global Marketing / Adgenics / Cabo Networks**
Florida affiliate spammers and bulletproof spam hosters

#5 **RetroCubes**
Web development, application development, and business training company that spams email appended lists, usually through ESPs that offer automated provisioning and services directed at small businesses.

#6 **Michael Persaud**
Long time snowshoe type spammer, raided by FBI then indicted in 2017 on federal wire fraud charges tied to his spamming operations.

#7 **Cyber World Internet Services/ e-Insites**
Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox. The company is owned or managed by Alvin Slocombe.

#8 **RR Media**
A high volume spam operation based in or run from Huntington Beach, CA, USA. The operation uses a variety of different names.

#9 **Kobeni Solutions**
High volume snowshoe spam operation based in Florida. The manager or owner of the company seems to be a Yair Shalev / . (Former?) partner-in-spam of ROKSO spammer Darrin Wohl. Son-in-law of ROKSO-listed spammer Dan Abramovich. Sued for fraud by the US

FTC in 2014.

Source: SpamHaus

Top countries with botnet

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

Source: SpamHaus

Top phishing countries

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