RelianceCyber

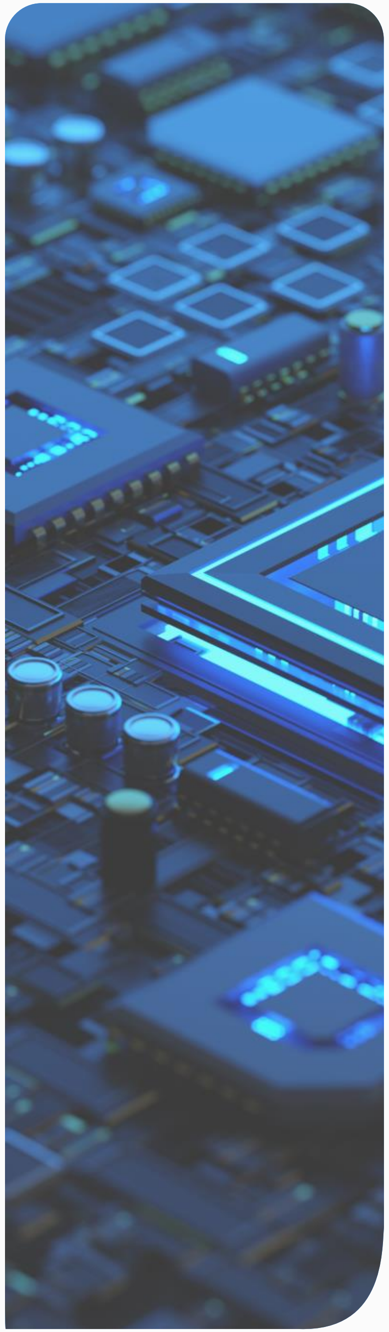
TLP: CLEAR

Threat Intelligence

WEEKLY BRIEFING

Written by: XDR Threat Intelligence Team

Date: 2024-08-30



RelianceCyber

Executive Summary

Reliance Cyber threat intelligence report details key areas such as newly observed threat actor activity, campaigns and vulnerabilities.

Their inclusion in this report does not necessarily mean that the client is affected, further vulnerability scanning and investigation would be required to establish exposure.

Vulnerability scores are accurate at the time of publishing but as many of these vulnerabilities are new it is quite likely that the CVSS scores may change over time.

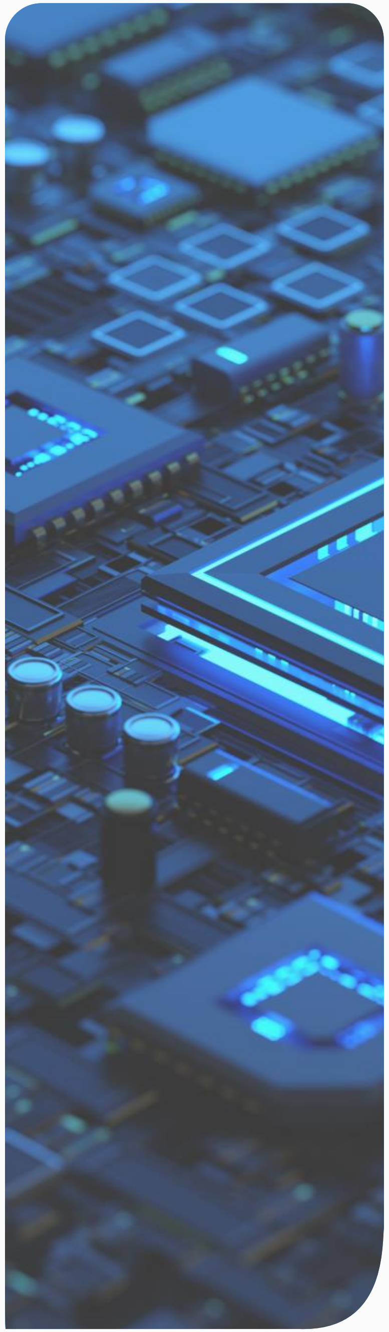
Please note that this information is based on the latest reports available and the situation may evolve.

In all cases, Reliance Cyber recommends that, where possible, you closely follow the manufacturer's latest advice to mitigate any vulnerabilities.

If you need any additional information on any of the advice in this week's Threat Intelligence Brief then please feel free to contact your Reliance Cyber Customer Success Manager.

TLP: CLEAR

Vulnerabilities



CISA Known Exploited Vulnerabilities (KEV)

CVE	Vendor	Product	Date Added
CVE-2021-31196	Microsoft	Exchange Server	21/08/2024
CVE-2022-0185	Linux	Kernel	21/08/2024
CVE-2021-33045	Dahua	IP Camera Firmware	21/08/2024
CVE-2021-33044	Dahua	IP Camera Firmware	21/08/2024
CVE-2024-39717	Versa	Director	23/08/2024
CVE-2024-7971	Google	Chromium V8	26/08/2024

For the benefit of the cybersecurity community and network defenders—and to help every organisation better manage vulnerabilities and keep pace with threat activity CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalogue.

CISA strongly recommends all organisations review and monitor the KEV catalogue and prioritise remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

These are the vulnerabilities added to the catalogue this week.

RelianceCyber

Weekly Vulnerability Summary

PRODUCT	CVE ID	CVSS C3 SCORE	Page
WordPress Woo Inquiry	CVE-2024-7854	10	7
WordPress WPML	CVE-2024-6386	9.9	8
Qualcomm Wi-Fi SON	CVE-2024-21473	9.8	9
TOTOLINK T10 AC1200 4.1.8cu.5207	CVE-2024-8162	9.8	10
Amazon AWS	ZDI-24-1177	9.8	11

Low	Medium	High	Critical
0.1– 3.9	4.0– 6.9	7.0 – 8.9	9.0 – 10.0

CVSS Key and Description

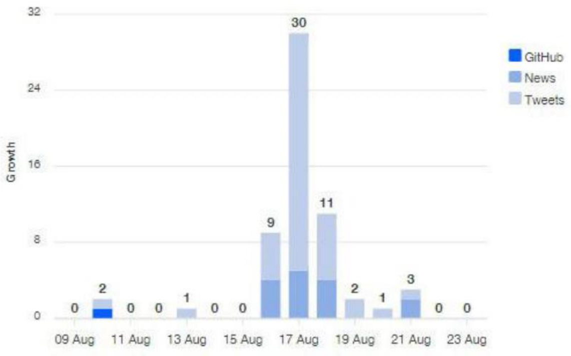
BASE METRIC CATEGORY	DESCRIPTION	OPTION
Attack Vector (AV)	This metric reflects the context by which vulnerability exploitation is possible.	Network Adjacent. Local, Physical
Attack Complexity (AC)	This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability	Low, High
Privileges Required (PR)	This metric describes the level of privileges an attacker must possess before successfully exploiting the vulnerability.	None, Low, High
User Interaction (UI)	This metric captures the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable component. None	None, Required
Scope (S)	The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope.	Unchanged, Changed
Confidentiality (C)	This metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability.	High, Low, None
Integrity (I)	This metric measures the impact to integrity of a successfully exploited vulnerability.	High, Low, None
Availability (A)	This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.	High, Low, None

The Github, News and Tweets graphic is used to indicate the amount of interest across these platforms in any particular vulnerability.

This lets us see which of the monitored channels has most active discussions about a vulnerability and also how much interest there is in a particular vulnerability over time.

It should be noted that this graphic is NOT showing any deep or dark web traffic regarding any vulnerabilities.

For more details about the CVSS Metrics, please see this resource: https://www.first.org/cvss/v3.1/specification-document

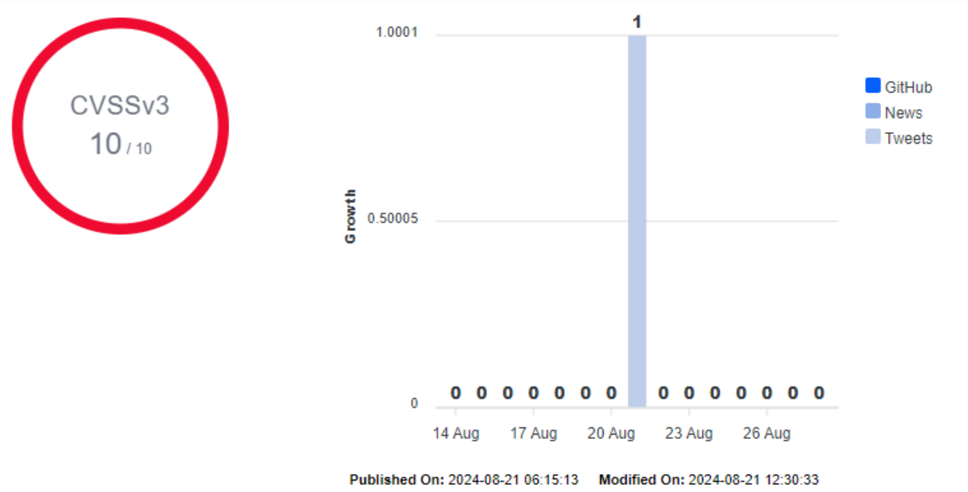


Published On: 2023-07-10 22:15:00 **Modified On:** 2023-07-18 18:19:00

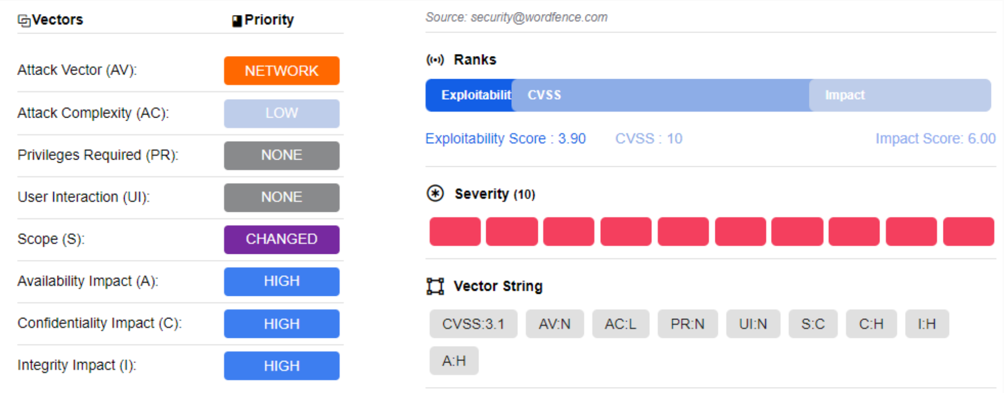
RelianceCyber

WordPress Woo Inquiry SQL Injection

CVE ID	CVE-2024-7854
SUMMARY	The Woo Inquiry plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 0.1 due to insufficient escaping on the user supplied parameter 'dbid' and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	No known patch available. It may be best to uninstall the affected software and find a replacement.
VENDOR RECOMMENDATION	https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/woo-inquiry/woo-inquiry-01-unauthenticated-sql-injection



Published On: 2024-08-21 06:15:13 **Modified On:** 2024-08-21 12:30:33



Vectors	Priority
Attack Vector (AV):	NETWORK
Attack Complexity (AC):	LOW
Privileges Required (PR):	NONE
User Interaction (UI):	NONE
Scope (S):	CHANGED
Availability Impact (A):	HIGH
Confidentiality Impact (C):	HIGH
Integrity Impact (I):	HIGH

Source: security@wordfence.com

Ranks

Exploitability Score : 3.90 CVSS : 10 Impact Score: 6.00

Severity (10)

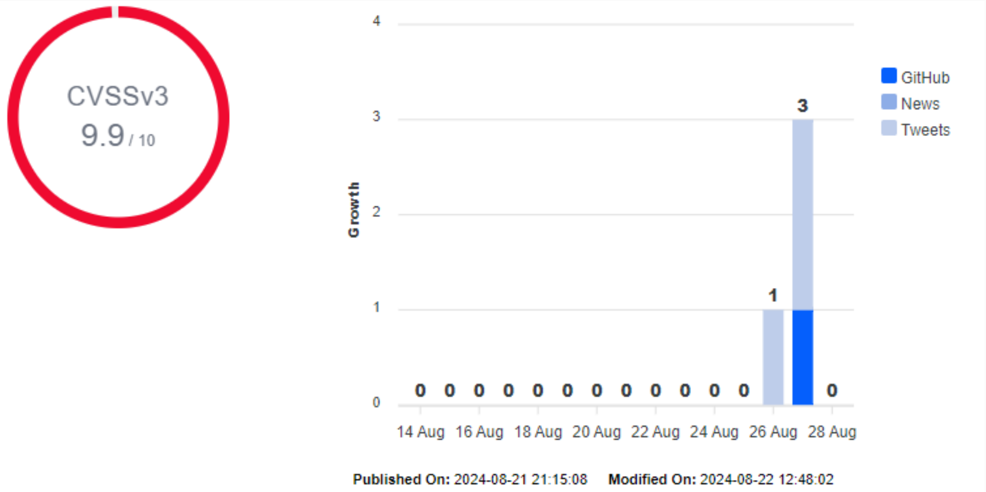
Vector String

CVSS:3.1 AV:N AC:L PR:N UI:N S:C C:H I:H A:H

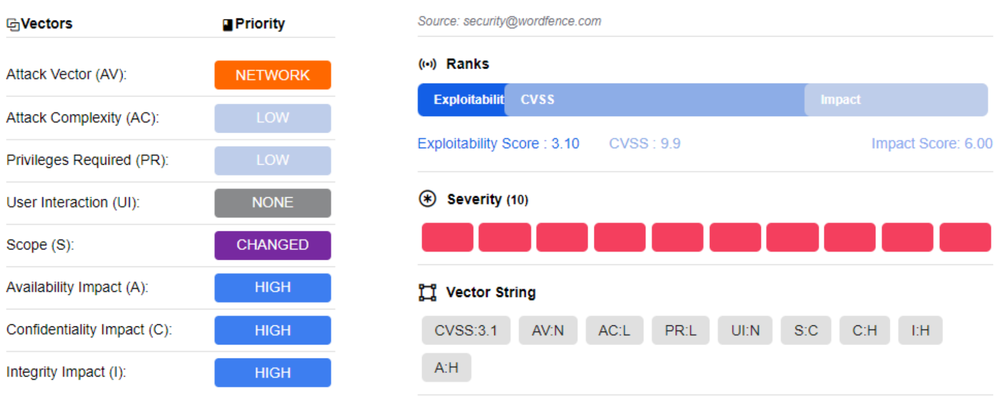
RelianceCyber

WordPress WPML Remote Code Execution

CVE ID	[CVE-2024-6386](CVE-2024-6386)
SUMMARY	The WPML plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.6.12 via the Twig Server-Side Template Injection. This is due to missing input validation and sanitisation on the render function. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server.
EXPLOITED IN THE WILD	YES
VENDOR SUGGESTED ACTION	Update to version 4.6.13, or a newer patched version
VENDOR RECOMMENDATION	https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/sitepress-multilingual-cms/wpml-multilingual-cms-4612-authenticatedcontributor-remote-code-execution-via-twig-server-side-template-injection



Published On: 2024-08-21 21:15:08 **Modified On:** 2024-08-22 12:48:02



Vectors	Priority
Attack Vector (AV):	NETWORK
Attack Complexity (AC):	LOW
Privileges Required (PR):	LOW
User Interaction (UI):	NONE
Scope (S):	CHANGED
Availability Impact (A):	HIGH
Confidentiality Impact (C):	HIGH
Integrity Impact (I):	HIGH

Source: security@wordfence.com

Ranks

Exploitability Score : 3.10 CVSS : 9.9 Impact Score: 6.00

Severity (10)

🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥

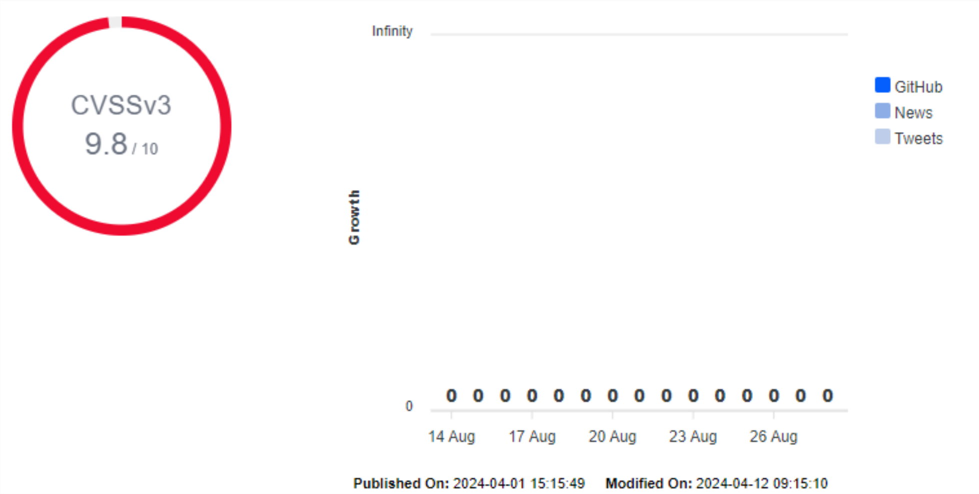
Vector String

CVSS:3.1 AV:N AC:L PR:L UI:N S:C C:H I:H A:H

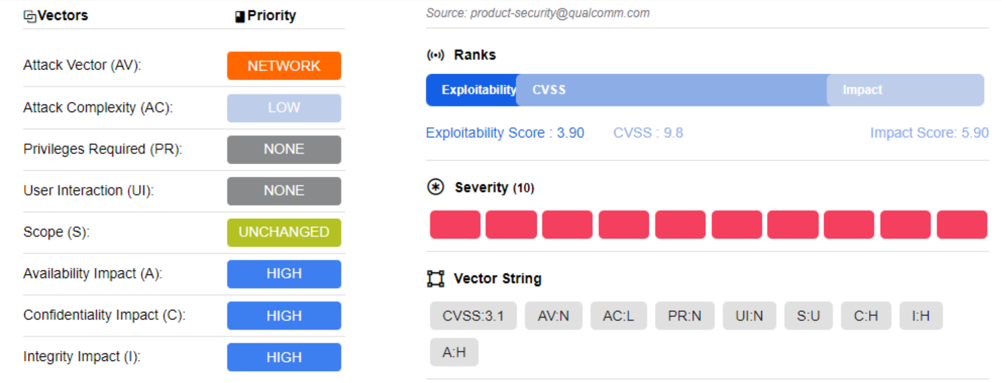
RelianceCyber

Qualcomm Wi-Fi SON Arbitrary Code Execution

CVE ID	CVE-2024-21473
SUMMARY	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of multiple Qualcomm chipsets. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Qualcomm LDB service. The issue results from the lack of proper validation of user-supplied data prior to further processing. An attacker can leverage this vulnerability to execute code in the context of root.
EXPLOITED IN THE WILD	YES
VENDOR SUGGESTED ACTION	No manufacturer advice at this time
VENDOR RECOMMENDATION	https://docs.qualcomm.com/product/publicresources/securitybulletin/april-2024-bulletin.html



Published On: 2024-04-01 15:15:49 **Modified On:** 2024-04-12 09:15:10



Vectors	Priority
Attack Vector (AV):	NETWORK
Attack Complexity (AC):	LOW
Privileges Required (PR):	NONE
User Interaction (UI):	NONE
Scope (S):	UNCHANGED
Availability Impact (A):	HIGH
Confidentiality Impact (C):	HIGH
Integrity Impact (I):	HIGH

Source: product-security@qualcomm.com

Ranks

Exploitability Score : 3.90 CVSS : 9.8 Impact Score: 5.90

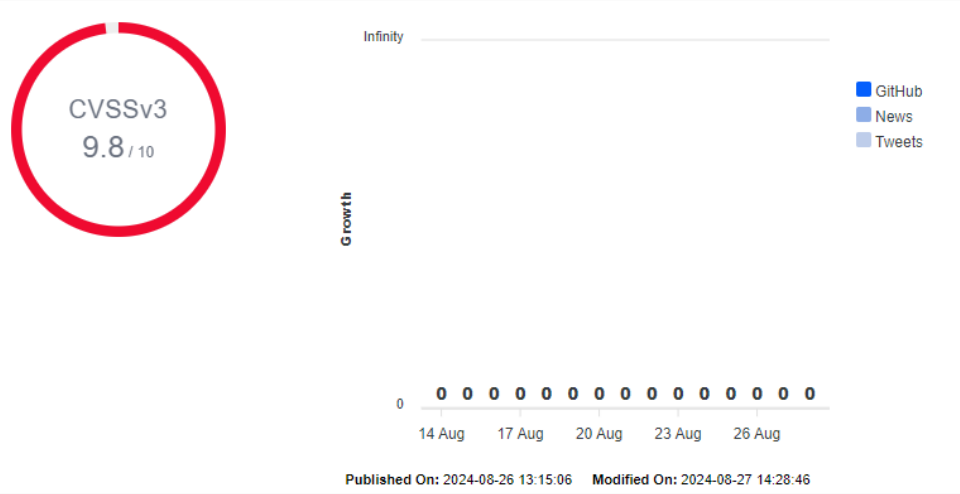
Severity (10)

Vector String

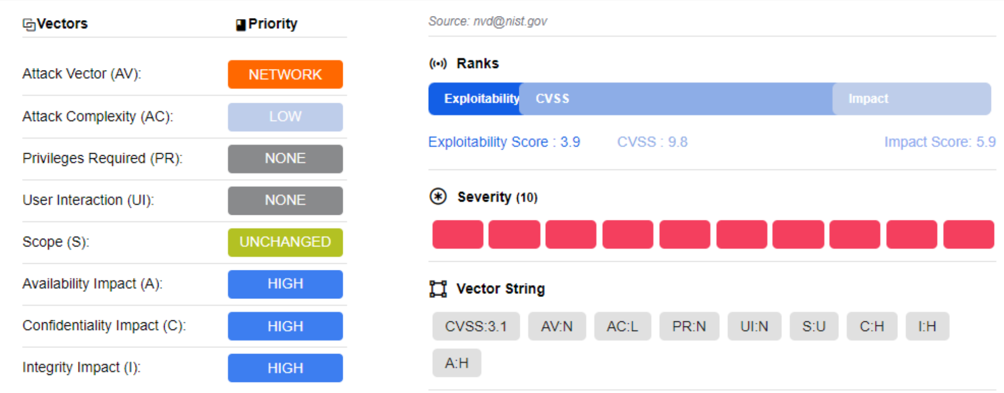
CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

TOTOLINK T10 AC1200 4.1.8cu.5207 Hard Coded Credentials

CVE ID	CVE-2024-8162
SUMMARY	A vulnerability classified as critical has been found in TOTOLINK T10 AC1200 4.1.8cu.5207. Affected is an unknown function of the file /squashfs-root/web_cste/cgi-bin/product.ini of the component Telnet Service. The manipulation leads to hard-coded credentials. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	No manufacturer advice at this time
VENDOR RECOMMENDATION	https://github.com/rohitburke/TOTOLINK



Published On: 2024-08-26 13:15:06 **Modified On:** 2024-08-27 14:28:46



Vectors	Priority
Attack Vector (AV):	NETWORK
Attack Complexity (AC):	LOW
Privileges Required (PR):	NONE
User Interaction (UI):	NONE
Scope (S):	UNCHANGED
Availability Impact (A):	HIGH
Confidentiality Impact (C):	HIGH
Integrity Impact (I):	HIGH

Source: nvd@nist.gov

Ranks

Exploitability Score : 3.9 CVSS : 9.8 Impact Score: 5.9

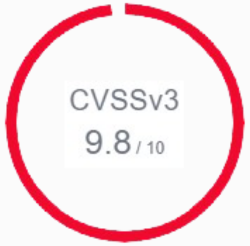
Severity (10)

Vector String

CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

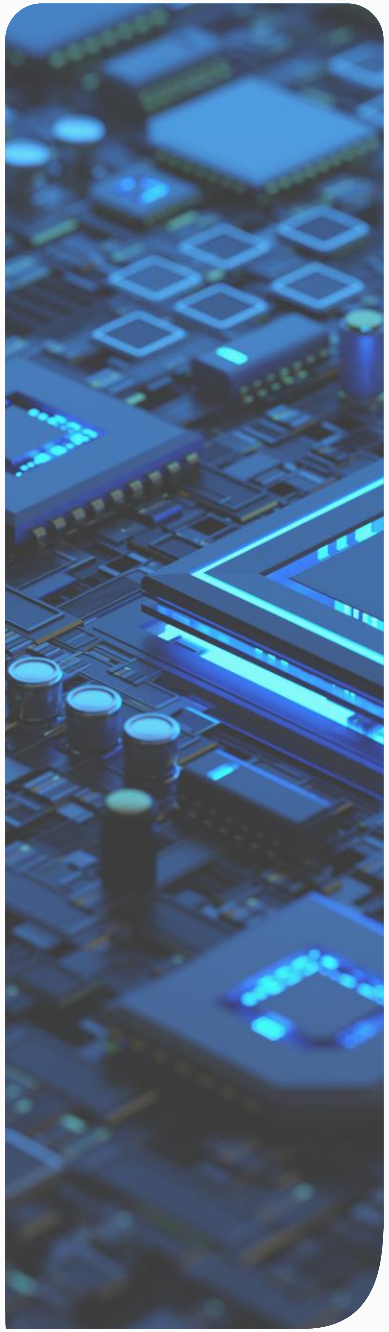
Amazon AWS Arbitrary Code Execution

CVE ID	ZDI-24-1177
SUMMARY	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Amazon AWS. Authentication is not required to exploit this vulnerability. The specific flaw exists within the installation of AWS Simple Storage Service. When installed from the official GitHub repository, the installation attempts to load a non-existent cloud resource that is vulnerable to takeover. An attacker can leverage this vulnerability to execute code on systems dependent on the cloud resource.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Amazon has issued an update to correct this vulnerability.
VENDOR RECOMMENDATION	https://github.com/aws-samples/amazon-es-service-recommended-alarms/commit/6115796183fc8cf4ef505f2efe9135b4566e1f9b



TLP: CLEAR

Threat Intelligence



BlackSuit Ransomware Deployed After 15 Days From Initial Access

The BlackSuit ransomware has been observed to be deployed approximately 15 days after initial access. This ransomware, which evolved from the Royal ransomware, typically gains initial access through phishing emails. Once inside the network, the attackers disable antivirus software and exfiltrate large amounts of data before deploying the ransomware.

The deployment process involves copying files over SMB to admin shares and executing them through RDP sessions. This method allows the attackers to move laterally within the network and maximise the impact of the ransomware.

RECOMMENDED ACTION

Phishing: Spot and report scam emails, texts, websites and calls

Phishing attacks: defending your organisation

Install, regularly update, and enable real time detection for antivirus

Add an email banner to emails from outside your organisation.

SEE ALSO

https://thedfirreport.com/2024/08/26/blacksuit-ransomware/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a

https://industrialcyber.co/cisa/cisa-and-fbi-issue-updated-alert-on-blacksuit-ransomware-targeting-critical-infrastructure-sectors/

https://www.globalsecuritymag.com/new-analysis-of-blacksuit-ransomware-group-from-reliaquest.html

RelianceCyber

Uber Fined $325 Million for Moving Driver Data From Europe to US

Uber has been fined €290 million (approximately $325 million) by the Dutch Data Protection Authority for transferring driver data from Europe to the U.S. without adequate protections. The fine was imposed due to violations of the General Data Protection Regulation (GDPR), which mandates strict data privacy and security measures.

Uber plans to appeal the fine, arguing that the data transfers occurred during a period of legal uncertainty regarding transatlantic data flows.

RECOMMENDED ACTION

Make sure that you are up to date with all current regulations

[ICO guide to the data protection principles]

[ICO UK GDPR guidance and resources]

SEE ALSO

https://www.bleepingcomputer.com/news/legal/uber-fined-325-million-for-moving-driver-data-from-europe-to-us/

https://www.morningstar.com/news/dow-jones/202408261563/uber-fined-325-million-in-europe-over-driver-data-transfers-to-the-us

https://mashable.com/article/uber-faces-324-million-fine-eu-mishandling-driver-data

RelianceCyber

China-linked APT Velvet Ant exploited Zero-Day to Compromise Cisco Switches

The China-linked Advanced Persistent Threat (APT) group known as Velvet Ant recently exploited a zero-day vulnerability in Cisco switches. This vulnerability, identified as CVE-2024-20399, is a command injection flaw in Cisco's NX-OS software.

Velvet Ant used this flaw to deploy custom malware on the affected devices, gaining unauthorised access to the underlying Linux operating system. This attack highlights the increasing sophistication of cyberespionage groups and the importance of promptly addressing security vulnerabilities.

RECOMMENDED ACTION

A full list of affected products and mitigations is available from Cisco at this URL;

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP

SEE ALSO

https://www.infosecurity-magazine.com/news/chinese-velvet-ant-cisco-0day/

https://securityaffairs.com/167423/apt/china-velvet-ant-zero-day-cisco-switches.html

https://www.csoonline.com/article/3493381/chinese-apt-group-velvet-ant-deployed-custom-backdoor-on-cisco-nexus-switches.html

https://www.sygnia.co/blog/china-threat-group-velvet-ant-cisco-zero-day/

Qilin Ransomware Caught Stealing Credentials Stored in Google Chrome

The Qilin ransomware group has recently been caught stealing credentials stored in Google Chrome. During a recent investigation, the Sophos X-Ops team discovered that Qilin used a PowerShell script to harvest credential data from Chrome browsers on infected endpoints. This tactic is unusual for ransomware groups and adds another layer of chaos to their attacks.

The attackers gained initial access through compromised credentials and then moved laterally within the network to deploy their credential-harvesting scripts. This method could have significant implications, as it means that not only must the affected organisation change all Active Directory passwords, but users may also need to change passwords for numerous third-party sites where credentials were stored in Chrome.

RECOMMENDED ACTION

This is a a stark reminder of the importance of robust security measures, including multi-factor authentication and regular monitoring for unusual activity. Reliance Cyber would also advise that you use industry-recognised password managers rather than storing passwords in browsers

SEE ALSO

https://news.sophos.com/en-us/2024/08/22/qilin-ransomware-caught-stealing-credentials-stored-in-google-chrome/

https://www.infosecurity-magazine.com/news/qilin-steal-credentials-google/

https://www.techradar.com/pro/security/google-chrome-details-can-be-stolen-by-this-clever-new-ransomware

https://cybernews.com/security/chrome-passwords-targeted-by-qilin-ransomware/

Jenkins RCE Attack

The recent Jenkins Remote Code Execution (RCE) attack is linked to a critical vulnerability identified as CVE-2024-23897. This vulnerability allows unauthenticated attackers to read arbitrary files from the Jenkins controller file system, which can lead to remote code execution. The flaw is due to the Jenkins Command-Line Interface (CLI) using the args4j library to parse command arguments, which doesn't disable a feature that replaces an '@' character followed by a file path with the file's contents

RECOMMENDED ACTION

This vulnerability has been actively exploited in ransomware campaigns, making it crucial for organisations using Jenkins to apply the latest security updates and patches. As published in the Jenkins Advisory

SEE ALSO

https://fortiguard.fortinet.com/outbreak-alert/jenkins-rce

https://community.fortinet.com/t5/FortiDevSec/Outbreak-Alert-Jenkins-RCE-Attack/ta-p/335766

https://gbhackers.com/critical-jenkins-vulnerabilities/

https://vulnera.com/newswire/critical-vulnerability-exposes-45k-jenkins-servers-to-rce-attacks

Thousands of Oracle NetSuite Sites at Risk of Exposing Customer Information

There has been a significant issue reported with Oracle NetSuite's SuiteCommerce platform. A misconfiguration in the way many sites are set up has left thousands of them vulnerable, potentially exposing sensitive customer information such as mailing addresses and phone numbers.

The problem lies in the way access controls are configured, allowing unauthorised users to access customer records through APIs. This isn't a flaw in the SuiteCommerce platform itself, but rather an issue with how some sites are configured.

To fix the problem, businesses need to tighten the security over these records. This can be done by changing the settings to make sure only authorized users can access the data, or by carefully reviewing and locking down specific fields that shouldn't be publicly accessible. In some cases, it might even be wise to temporarily take the affected sites offline until these issues are resolved.

RECOMMENDED ACTION

If you use NetSuite, it might be a good idea to review your security settings and ensure your site isn't affected.

SEE ALSO

https://www.scmagazine.com/news/thousands-of-oracle-netsuite-sites-said-to-be-exposing-customer-data

https://www.msn.com/en-gb/money/technology/thousands-of-oracle-netsuite-erp-websites-found-leaking-private-customer-information/ar-AA1oVraZ

https://www.csoonline.com/article/3487234/thousands-of-netsuite-stores-leak-sensitive-data-due-to-access-control-misconfiguration.html

https://www.darkreading.com/application-security/oracle-netsuite-ecommerce-sites-expose-customer-data

RelianceCyber

Windows Driver Zero-Day Exploited by Lazarus Hackers to Install Rootkit

The Lazarus hacking group, which is linked to North Korea, recently exploited a zero-day vulnerability in the Windows AFD.sys driver to install a rootkit known as FUDModule. This vulnerability, tracked as CVE-2024-38193, allowed the attackers to gain elevated privileges and bypass security measures.

Microsoft has since patched this flaw in their August 2024 update.

RECOMMENDED ACTION

It's a significant reminder of the importance of keeping systems patched and up to date to protect against such sophisticated threats.

Software updates and other advice is available from https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193

SEE ALSO

https://www.bleepingcomputer.com/news/microsoft/windows-driver-zero-day-exploited-by-lazarus-hackers-to-install-rootkit/

https://winbuzzer.com/2024/08/20/north-korean-hackers-use-windows-zero-day-to-deploy-rootkit-xcxwbn/

https://arstechnica.com/security/2024/08/windows-0-day-was-exploited-by-north-korea-to-install-advanced-rootkit/

RelianceCyber

North Korea's BlueNoroff Targets macOS with TodoSwift Malware

The BlueNoroff group, a subgroup of North Korea's Lazarus Group, has been targeting macOS systems with a new malware called TodoSwift. This malware is disguised as a PDF related to Bitcoin, tricking users into downloading it. Once installed, TodoSwift can steal cryptocurrency and bypass international sanctions.

The malware is distributed as a signed file named TodoTasks, which contains a dropper component that displays a weaponised PDF to victims and downloads a second-stage binary. This second-stage binary retrieves system information and communicates with a command-and-control server.

RECOMMENDED ACTION

It's a sophisticated attack, so it's crucial to be cautious with unexpected emails and downloads, especially those related to cryptocurrency.

NCSC Phishing: Spot and report scam emails, texts, websites and calls

SEE ALSO

https://cyware.com/news/new-macos-malware-todoswift-linked-to-north-korean-hacking-groups-2fc097d8

https://9to5mac.com/2023/11/07/bluenoroff-targets-mac-users-with-new-malware/

https://www.bankinfosecurity.com/north-koreas-bluenoroff-group-targets-macos-systems-a-22149

https://www.hackread.com/lazarus-bluenoroff-apt-macos-objcshellz-malware/

RelianceCyber

The Mad Liberator Targets AnyDesk Users with Fake Windows Updates

The Mad Liberator ransomware group has been targeting AnyDesk users by disguising their attacks as fake Windows updates. This group uses social engineering tactics to gain access to devices through AnyDesk, a legitimate remote-access tool. Once they have access, they deploy a fake Windows update screen to hide their malicious activities.

The attackers focus on data exfiltration and sometimes use double extortion tactics, where they steal data and then encrypt the victim's systems, threatening to leak the stolen data unless a ransom is paid. It's a sophisticated approach that exploits the trust users have in familiar software like AnyDesk.

RECOMMENDED ACTION

If you use AnyDesk, it's crucial to be cautious about unexpected connection requests and to verify the source before granting access. Implementing security measures, such as allowing connections only from specific devices, can also help prevent such attacks.

SEE ALSO

https://www.theregister.com/2024/08/15/mad_liberator_extortion/

https://news.sophos.com/en-us/2024/08/13/dont-get-mad-get-wise/

https://cyware.com/news/mad-liberator-gang-uses-fake-windows-update-screen-to-hide-data-theft-cedb2f8b/

https://izoologic.com/hacking/mad-liberator-a-new-threat-group-that-uses-fake-windows-update/

RelianceCyber

RELIANCECYBER.COM