RelianceCyber

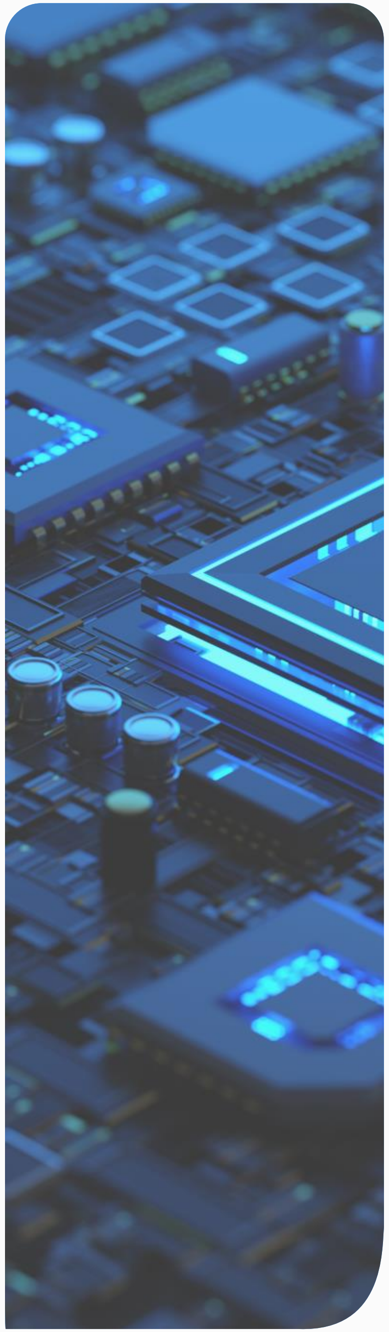
TLP: CLEAR

Threat Intelligence

WEEKLY BRIEFING

Written by: XDR Threat Intelligence Team

Date: 2024-09-06



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.

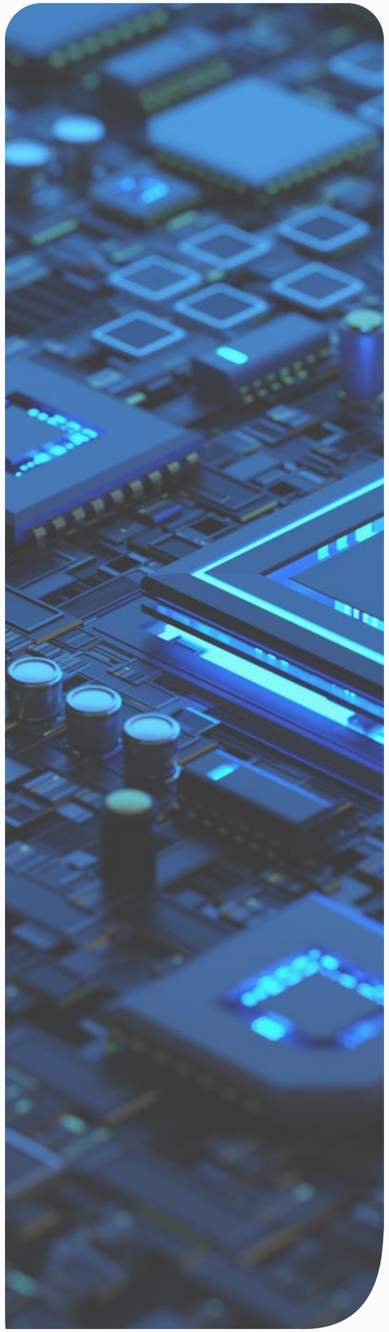
Please note that this information is based on the latest reports available and the situation may evolve.

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



RelianceCyber

CISA Known Exploited Vulnerabilities (KEV)

CVE	Vendor	Product	Date Added
CVE-2024-7965	Google	Chromium V8	28/08/2024
CVE-2024-7262	Kingsoft	WPS Office	03/09/2024
CVE-2021-20124	DrayTek	VigorConnect	03/09/2024
CVE-2021-20123	DrayTek	VigorConnect	03/09/2024

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
IBM	CVE-2024-45076	9.8	7
WhatsUp Gold	CVE-2024-6670	9.8	8
WhatsUp Gold	CVE-2024-6671	9.8	9
Zyxel	CVE-2024-7261	9.8	10
WordPress	CVE-2024-7857	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

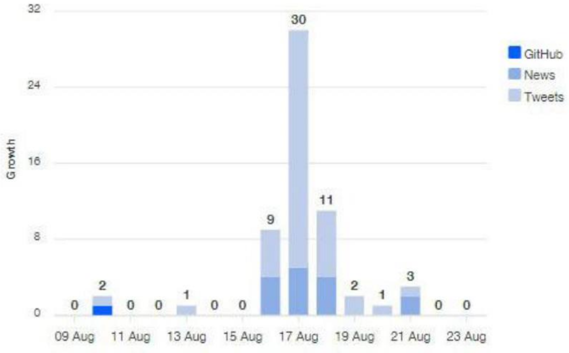
BASE METRIC CATEGORY	DESCRIPTION	OPTION
Attack Vector (AV)	This metric reflects the context by which vulnerability exploitation is possible.	Network Adjacent. Local, Physical
Attack Complexity (AC)	This metric describes the conditions beyond the attacker's control that must exist in order to exploit 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

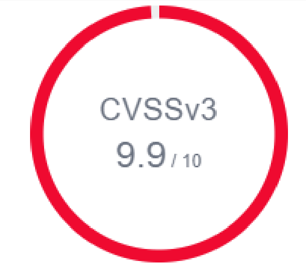


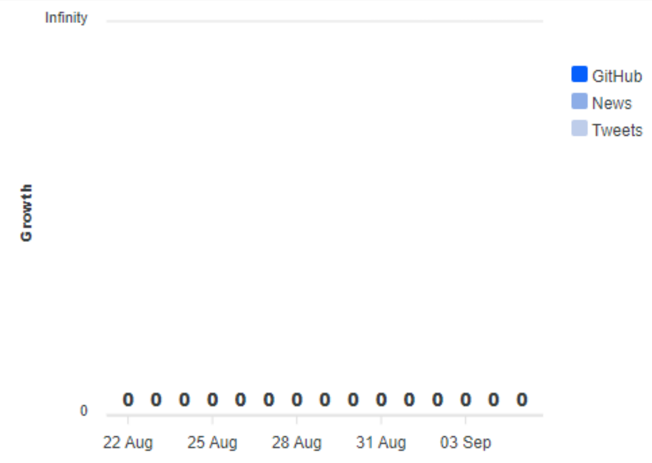
Published On: 2023-07-10 22:15:00 **Modified On:** 2023-07-18 18:19:00

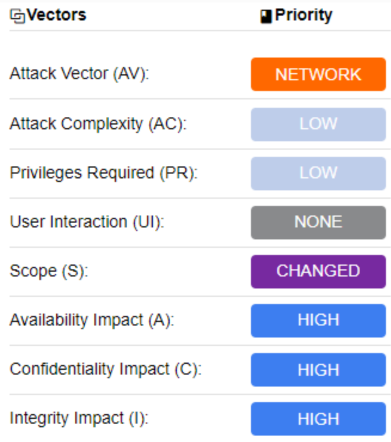
RelianceCyber

IBM webMethods Integration vulnerability

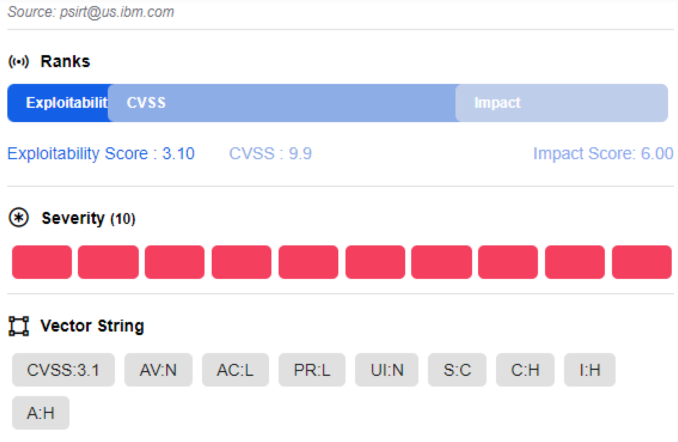
CVE ID	CVE-2024-45076
SUMMARY	CVE-2024-45076 is a critical vulnerability in IBM webMethods Integration 10.15 that allows an authenticated user to upload and execute arbitrary files on the underlying operating system. This vulnerability has a CVSS score of 9.9, indicating its severe impact and urgency. The SOCRadar Vulnerability Risk Score (SVRS) for this CVE is 0, which means that it is not currently being actively exploited or associated with any known threat actors or malware.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Install Corefix 14 of Integration Server using Update Manager
VENDOR RECOMMENDATION	[Security Bulletin: Multiple vulnerabilities in IBM webMethods Integration](#)







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: psirt@us.ibm.com

Ranks

Exploitability Score : 3.10 CVSS : 9.9 Impact Score: 6.00

Severity (10)

🟥 🟥 🟥 🟥 🟥 🟥 🟥 🟥 🟥 🟥

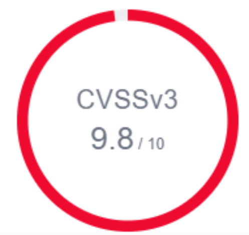
Vector String

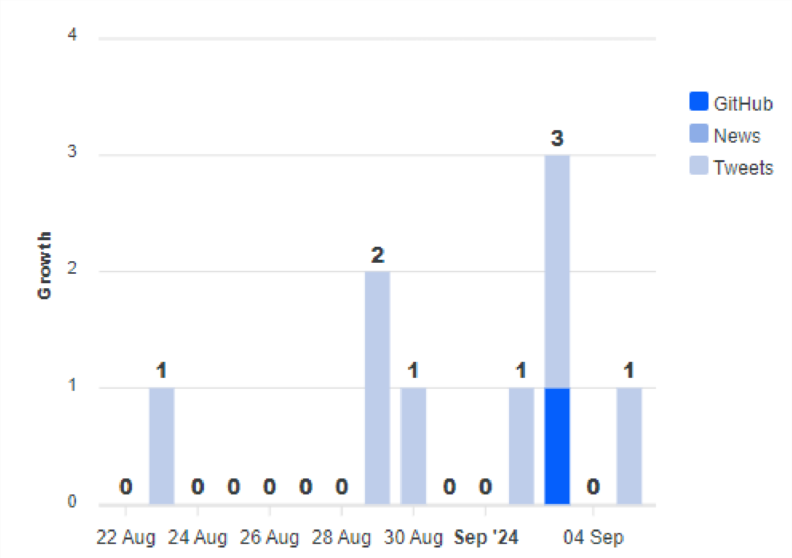
CVSS:3.1 AV:N AC:L PR:L UI:N S:C C:H I:H A:H

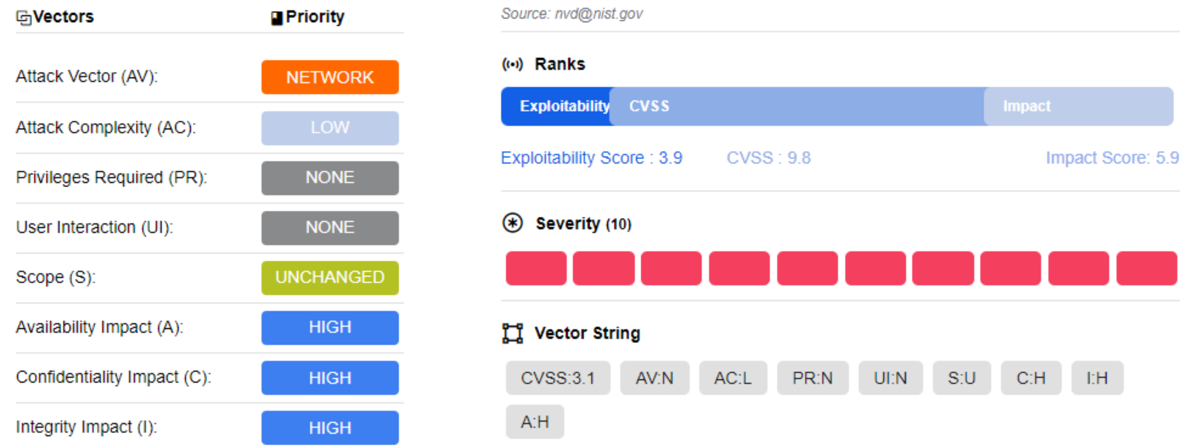
RelianceCyber

WhatsUp Gold SQL Injection vulnerability

CVE ID	CVE-2024-6670
SUMMARY	CVE-2024-6670 is a SQL Injection vulnerability in WhatsUp Gold versions released before 2024.0.0. This vulnerability allows an unauthenticated attacker to retrieve the users' encrypted password. The SVRS for this vulnerability is 91, indicating a critical severity level and necessitating immediate action.
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	We strongly encourage all WhatsUp Gold customers on every older version to upgrade their environment as soon as possible. For clarity, if you are running a version older than version 24.0.0 and you don't upgrade to the patched version, you will continue to be vulnerable. All customers with an active service agreement are eligible to upgrade to the latest version free of charge.
VENDOR RECOMMENDATION	[WhatsUp Gold Security Bulletin– August 2024 - Progress Community]()







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)

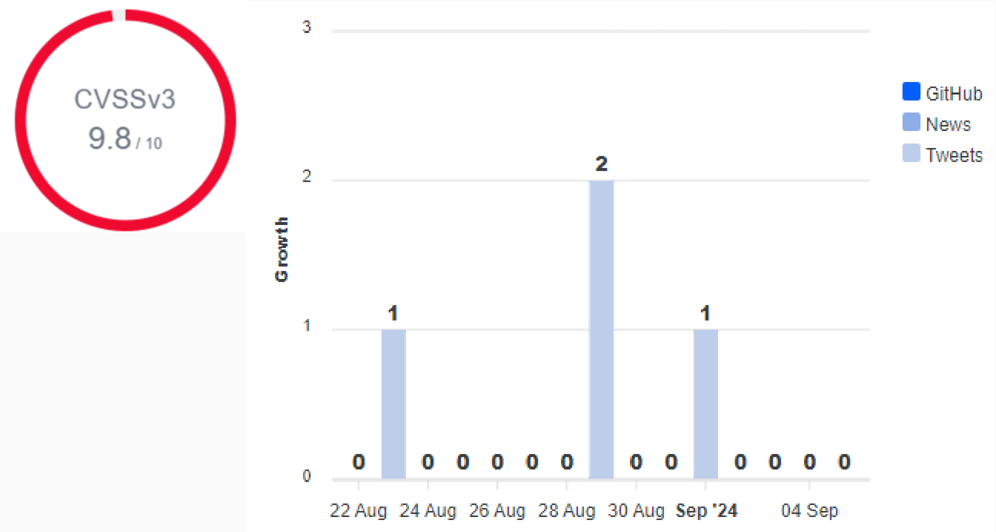
Vector String

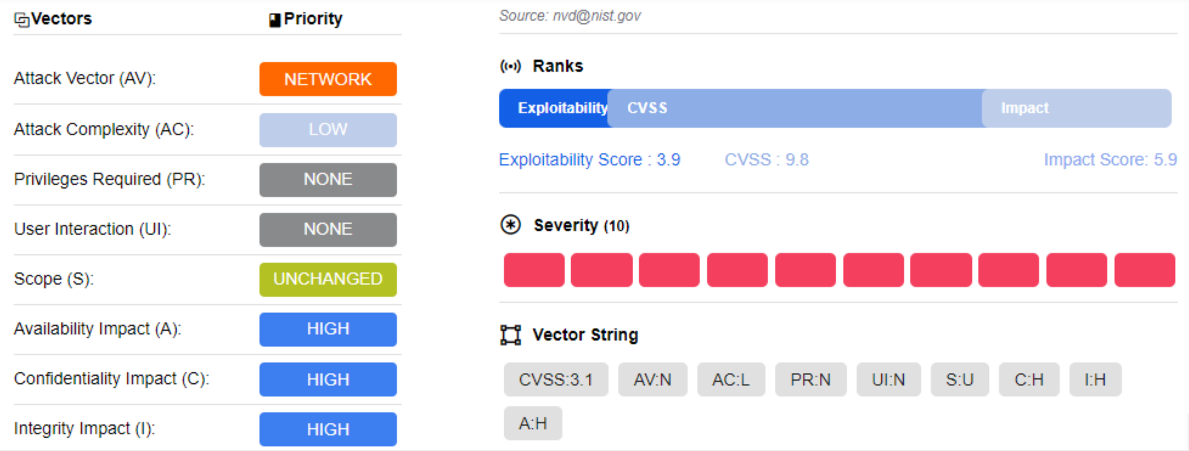
CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

RelianceCyber

WhatsUp Gold SQL Injection vulnerability

CVE ID	CVE-2024-6671
SUMMARY	CVE-2024-6671 is a SQL Injection vulnerability in WhatsUp Gold versions released before 2024.0.0. This vulnerability allows an unauthenticated attacker to retrieve the user's encrypted password if the application is configured with only a single user. The CVSS score of 9.8 and the SVRS of 87 indicate that this vulnerability is critical and requires immediate attention.
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	We strongly encourage all WhatsUp Gold customers on every older version to upgrade their environment as soon as possible. For clarity, if you are running a version older than version 24.0.0 and you don't upgrade to the patched version, you will continue to be vulnerable. All customers with an active service agreement are eligible to upgrade to the latest version free of charge.
VENDOR RECOMMENDATION	[WhatsUp Gold Security Bulletin– August 2024 - Progress Community]()





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 CVSS Impact

Exploitability Score : 3.9 CVSS : 9.8 Impact Score: 5.9

Severity (10)

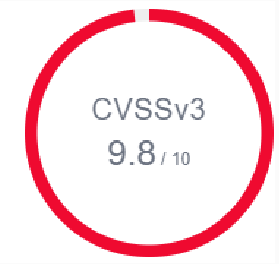
Vector String

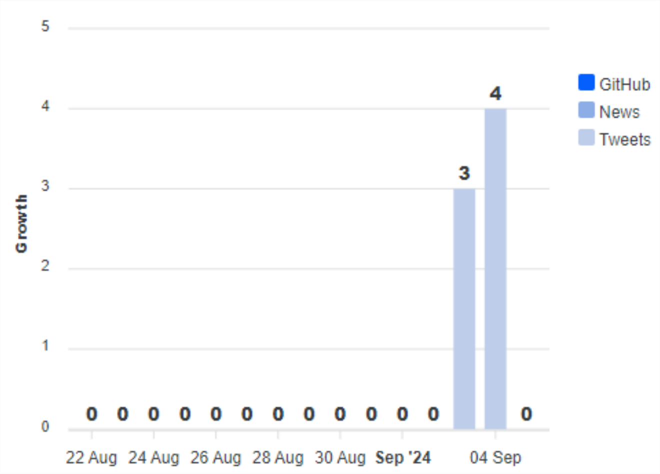
CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

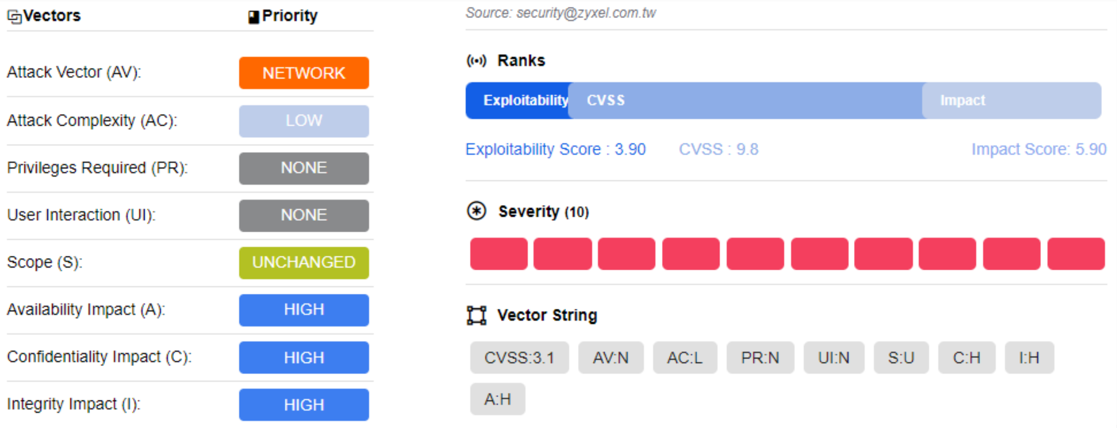
RelianceCyber

Zyxel Vulnerability

CVE ID	CVE-2024-7261
SUMMARY	CVE-2024-7261 is a critical vulnerability in Zyxel network devices that allows unauthenticated attackers to execute arbitrary commands on the affected systems. The vulnerability stems from improper neutralization of special elements in the "host" parameter of the CGI program in the firmware of these devices.
EXPLOITED IN THE WILD	No
VENDOR SUGGESTED ACTION	Apply patches.
VENDOR RECOMMENDATION	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-aps-and-security-router-devices-09-03-2024







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: security@zyxel.com.tw

Ranks

Exploitability CVSS Impact

Exploitability Score : 3.90 CVSS : 9.8 Impact Score: 5.90

Severity (10)

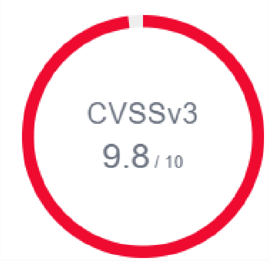
Vector String

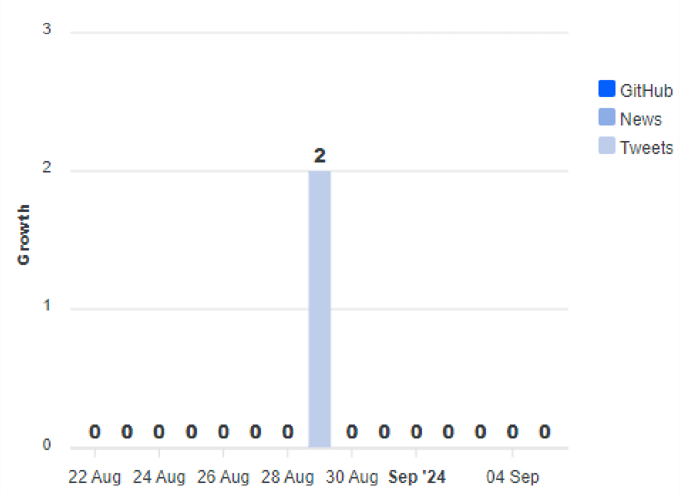
CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

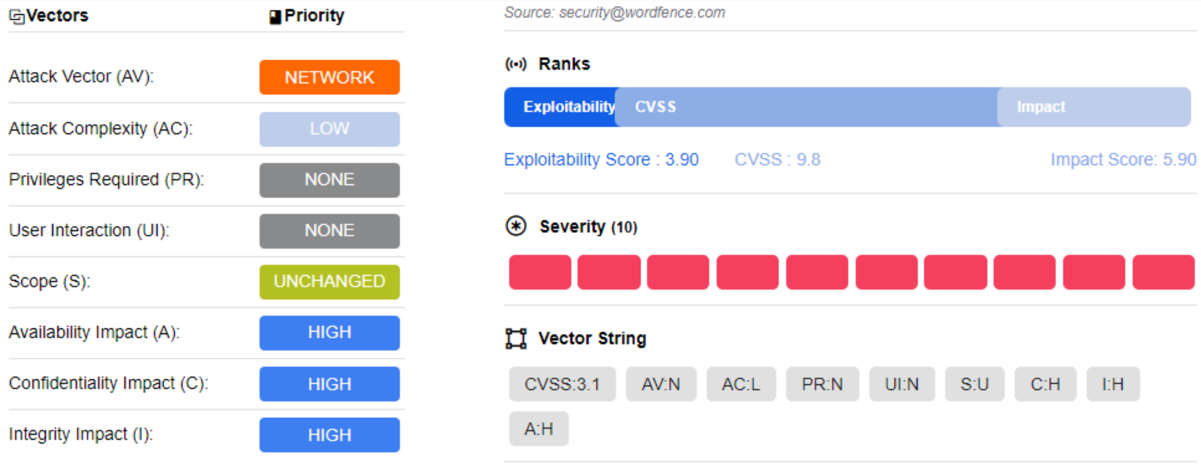
RelianceCyber

WordPress SQL Injection vulnerability

CVE ID	CVE-2024-7857
SUMMARY	CVE-2024-7857 is a second-order SQL injection vulnerability in the Media Library Folders plugin for WordPress. It allows authenticated attackers with subscriber-level access or higher to execute arbitrary SQL queries on the database, potentially leading to sensitive information disclosure. The SVRS of 30 indicates a moderate risk, requiring attention and appropriate mitigation measures.
EXPLOITED IN THE WILD	No
VENDOR SUGGESTED ACTION	Update to version 8.2.3, or a newer patched version
VENDOR RECOMMENDATION	https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/media-library-plus/media-library-folders-822-authenticated-subscriber-second-order-sql-injection







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: security@wordfence.com

Ranks

Exploitability Score : 3.90 CVSS : 9.8 Impact Score: 5.90

Severity (10)

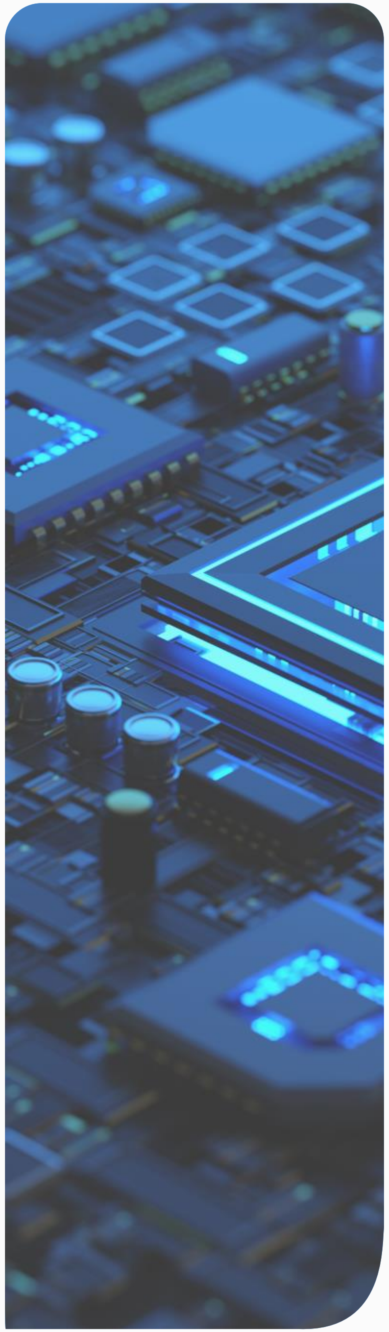
Vector String

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

RelianceCyber

TLP: CLEAR

Threat Intelligence



RelianceCyber

Threat Actors Use Godzilla Web shell to Exploit Atlassian Confluence CVE-2023-22527 for Remote Execution

On August 30, 2024, Trend Micro identified a new attack vector exploiting CVE-2023-22527, a critical vulnerability in older Atlassian Confluence versions that allows unauthenticated remote code execution. The exploit involves Godzilla, a fileless malware developed by the Chinese-speaking user "BeichenDream," which functions as a web shell and a backdoor. Godzilla uses Advanced Encryption Standard (AES) encryption to operate entirely in-memory and avoid traditional antivirus detection, enabling unauthorized server access and command execution.

The attack exploits CVE-2023-22527 by executing an Object-Graph Navigation Language (OGNL) object in a designed velocity.struts2.context. This action installs the Godzilla web shell on the compromised Atlassian server. Godzilla uses Java Reflection to access and manipulate private fields and methods and to scan for crucial threads in Tomcat's architecture. It then dynamically loads the MemGodValueShell class from Base64-encoded strings. This class enables the injection of a custom valve into Tomcat's pipeline, granting unauthorized access and control over the server.

RECOMMENDED ACTION

Reliance Cyber recommends applying the patch to mitigate this threat.

SEE ALSO

https://www.trendmicro.com/en_us/research/24/h/godzilla-fileless-backdoors.html

https://cybersecuritynews.com/godzilla-fileless-backdoor-exploits/#google_vignette

New Ransomware-as-a-Service Known As Cicada3301 Targeting VMware ESXi Systems

Cicada3301 Ransomware Group, a new ransomware-as-a-service (Raas) group), has been targeting VMware ESXi systems using Rust-based malware. According to a report by Truesec on August 30, 2024, Cicada3301 uses ransomware with functionalities and features that overlap with that used by the ALPHV ransomware group, potentially indicating a rebrand of ALPHV. Bleeping Computer also reported that Cicada3301 first promoted its operation on the RAMP cybercrime forum in June 2024 and listed 19 victims at the time of writing.

Cicada3301 employs double-extortion techniques, encrypting files and threatening to leak stolen data to coerce victims into paying ransoms. Similar to ALPHV, the Cicada3301 ransomware strain uses the ChaCha20 encryption algorithm, shutting down virtual machines on VMware ESXi systems and wiping snapshots before encrypting the data. The ransomware's infection chain begins with initial access, often facilitated by the Brutus botnet, which brute-forces credentials for remote access solutions like ScreenConnect. After gaining access, the ransomware encrypts specific file types, using a unique key to decrypt a ransom note, and then demands payment for the data's recovery.

RECOMMENDED ACTION

Reliance Cyber recommends review of the mitigations section for the Initial Access Technique : Valid Accounts. General Ransomware Mitigation Techniques are also recommended.

SEE ALSO

https://www.truesec.com/hub/blog/dissecting-the-cicada

https://www.bleepingcomputer.com/news/security/cicada3301-ransomwares-linux-encryptor-targets-vmware-esxi-systems/

https://www.cicada3301official.com/pages/content/images/3301-statement-september-1-2024.jpg

Threat Actors Exploit Github Comments to Deploy Lumma Stealer

Threat actors are distributing Lumma Stealer malware via GitHub by posting fake fixes in project comments. According to a report by Bleeping Computer on August 31, 2024, over 29,000 malicious comments have been posted on GitHub, leading victims to download a password-protected archive containing Lumma Stealer.

The infection chain starts with users clicking on a link in the GitHub comments pretending to be a solution to their questions. This link leads them to a download page for an archive named 'fix.zip'. The archive includes DLL files and an executable that, when run, steals data from various browsers and crypto wallets. This information is collected and sent back to the threat actors through their command-and-control (C2) servers. GitHub staff is actively working to remove these malicious posts, but many users have already fallen victim to them.

RECOMMENDED ACTION

Reliance Cyber recommends raising awareness of this activity and exercising caution when reviewing external links.

SEE ALSO

https://www.reddit.com/r/Malware/comments/1f2n1h4/psa_lummac2_trojan_stealer_spreading_on_github/

https://www.bleepingcomputer.com/news/security/github-comments-abused-to-push-password-stealing-malware-masked-as-fixes/

Velvet Ant Exploits CVE-2024-20399 in Cisco Switches to Deploy VELVETSHELL Malware

On August 22, 2024, cybersecurity firm Sygnia provided an update to their July 2024 report detailing how the China-nexus threat group "Velvet Ant" exploited CVE-2024-20399 in Cisco NX-OS Software to deploy a customized malware known as VELVETSHELL. Previously, in the first iteration of the report published in July 2024, the malware deployed on victim entities was unknown.

Researchers analyzed the reconstructed VELVETSHELL malware and found that it combines two open-source tools, TinyShell, a Unix backdoor, and 3proxy, a proxy tool, into a single customized version. While these tools were previously used independently for malicious activities, in this case, they were integrated into one binary.

In July 2024, Cisco previously patched CVE-2024-20399, which is a command injection flaw arising from improper validation of input parameters in command-line interface (CLI) commands. CVE-2024-20399 affects vulnerable NX-OS software MDS 9000 Series, and Nexus 3000, 5500, 5600, 6000, 7000, and 9000 Series.

The attack chain began when Velvet Ant acquired administrator credentials to access Cisco Nexus switch management consoles. Once the threat actors accessed the switches, they exploited CVE-2024-20399 to "escape the NX-OS CLI context" and execute commands on the Linux operating system. Velvet Ant installed VELVETSHELL on the OS, the execution of which remained undetectable by standard security tools, as the targeted switches restrict users from accessing the underlying operating system, which makes scanning for indicators of compromise "nearly impossible". Velvet Ant then copied the legitimate curl binary, renaming it ufdm to mimic a legitimate process on Cisco Nexus switch appliances. They used the LD_PRELOAD environment variable to load ufdm.so, injecting their malicious code into the renamed process and gaining control over the device's execution flow. This technique allowed them to stay undetected while using the ps and netstat commands to monitor system processes and network activity, and to exfiltrate data from the target systems. After confirming their malware was running as intended, Velvet Ant took steps to erase their traces by deleting the files ufdm and ufdm.so.

Recent cyber threat activity involving Velvet Ant reveals a pattern of targeting Cisco and F5 BIG-IP devices, demonstrating a tendency for targeting network infrastructure components that offer control over network traffic and security. These targets are attractive due to their critical roles in network security and management, making them valuable for persistent network access, defense evasion, and data exfiltration. Additionally, previous campaigns act as an incentive and proof-of-concept for threat actors seeking to conduct cyberespionage.

Velvet Ant Exploits CVE-2024-20399 in Cisco Switches to Deploy VELVETSHELL Malware

Network appliances such as network switches often have limited visibility, logging capabilities, and support for traditional security solutions. Because the internal workings of many appliances are not fully visible, they are often misconfigured or not properly patched, turning each piece of hardware or software into a potential attack surface that an adversary can exploit to gain access to a target's network. Based on a combination of these factors and existing trends related to the exploitation of network appliances, we assess it is almost certain that the exploitation of these devices will continue. Organizations should consider these factors when installing network appliances in order to avoid introducing vulnerable systems into their attack surface.

Recommendations

To effectively detect the provided Indicators of Compromise (IOCs), security practitioners should focus on implementing file integrity monitoring that can help detect the creation or modification of suspicious files in critical directories like /bootflash and /root, ensuring any unauthorized changes are immediately flagged. Behavioral monitoring and anomaly detection are essential to identify abnormal activities, such as unexpected file executions or the loading of malicious libraries, which can indicate the presence of renamed tools or other threats.

There are two additional priority mitigations for defenders operating affected devices in response to this campaign. First, given that stolen credentials were the initial access vector, it is important to ensure credential hygiene and follow practices such as monitoring and rotating credentials frequently, especially for administrative-level devices. Secondly, if defenders have not already done so they should ensure they have patched CVE-2024-20399.

Sources

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

https://thehackernews.com/2024/08/chinese-hackers-exploit-zero-day-cisco.html

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

https://www.zenarmor.com/docs/network-security-tutorials/what-is-network-visibility

https://www.auvik.com/franklyit/blog/network-visibility-guide/

RelianceCyber

RELIANCECYBER.COM