RelianceCyber

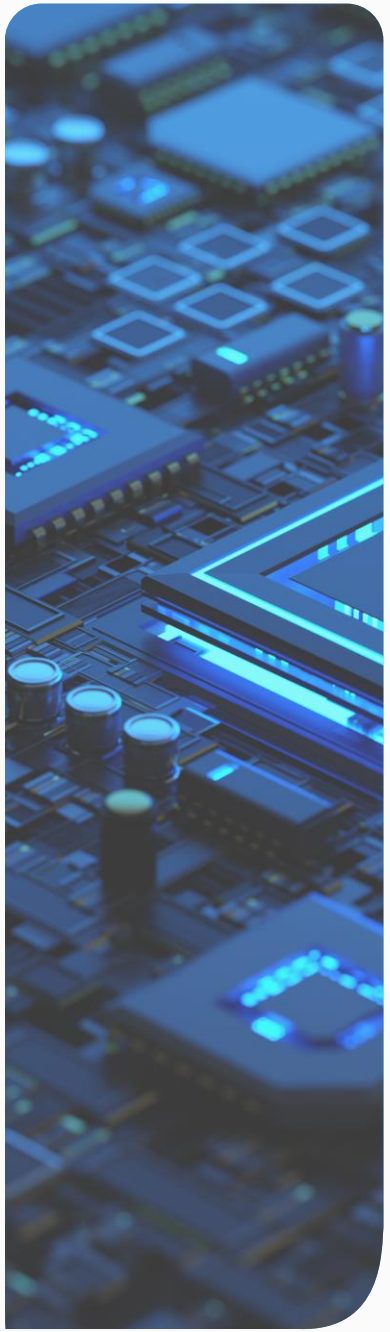
TLP: CLEAR

Threat Intelligence

WEEKLY BRIEFING

Written by: XDR Threat Intelligence Team

Date: 2024-09-13



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.

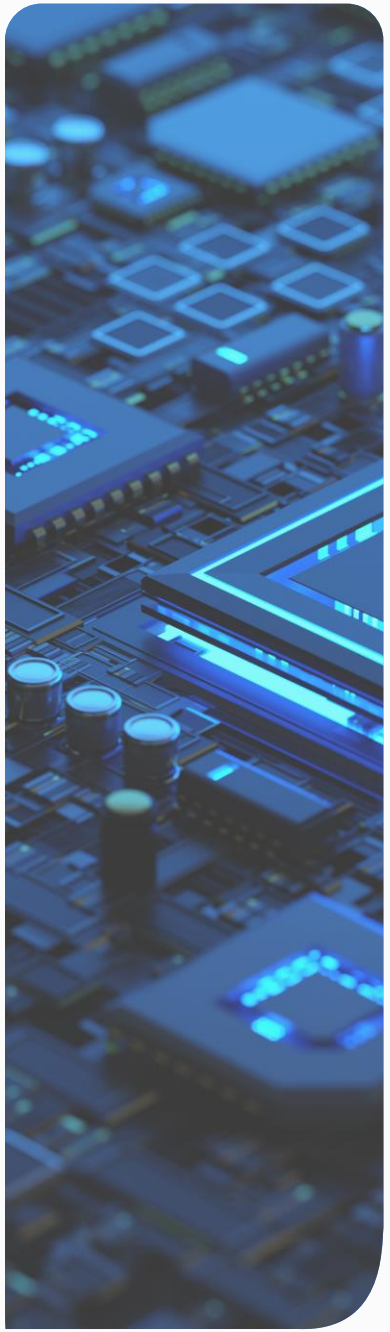
In all cases, Reliance Cyber recommends that, where possible, you closely follow the manufacturer's latest advice to mitigate any vulnerabilities.

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.

RelianceCyber

TLP: CLEAR

Vulnerabilities



RelianceCyber

CISA Known Exploited Vulnerabilities (KEV)

CVE	Vendor	Product	Date Added
CVE-2024-40766	SonicWall	SonicOS	09/09/2024
CVE-2017-1000253	Linux	Kernel	09/09/2024
CVE-2016-3714	ImageMagick	ImageMagick	09/09/2024
CVE-2024-38217	Microsoft	Windows	10/09/2024
CVE-2024-38014	Microsoft	Windows	10/09/2024
CVE-2024-43491	Microsoft	Windows	10/09/2024
CVE-2024-38226	Microsoft	Publisher	10/09/2024

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
Progress LoadMaster	CVE-2024-7591	10	7
Ivanti EPM	CVE-2024-29847	10	8
Kibana Amazon Bedrock Connector	CVE-2024-37288	9.9	9
Veeam VSPC server	CVE-2024-38650	9.9	10
Veeam VSPC server	CVE-2024-39714	9.9	11
Zyxel NAS326	CVE-2024-6342	9.8	12

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

RelianceCyber

CVSS Key and Description

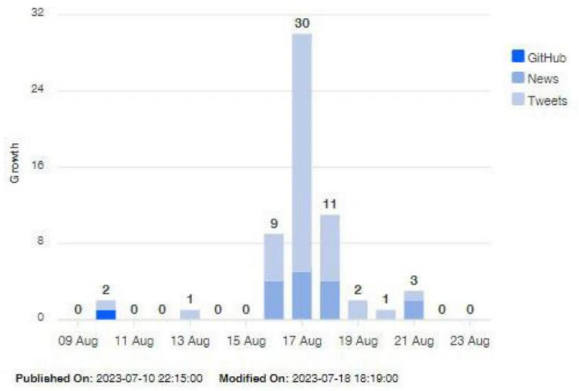
BASE METRIC CATEGORY	DESCRIPTION	OPTION
Attack Vector (AV)	This metric reflects the context by which vulnerability exploitation is possible.	Network Adjacent. Local, Physical
Attack Complexity (AC)	This metric describes the conditions beyond the attacker's control that must exist in order to exploit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

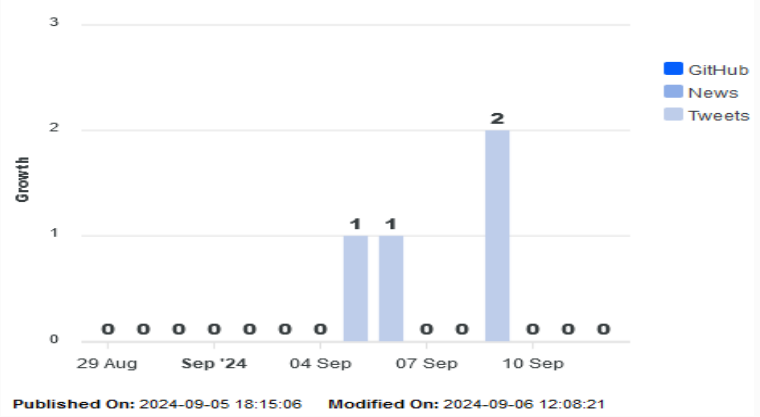
For more details about the CVSS Metrics, please see this resource: https://www.first.org/cvss/v3.1/specification-document

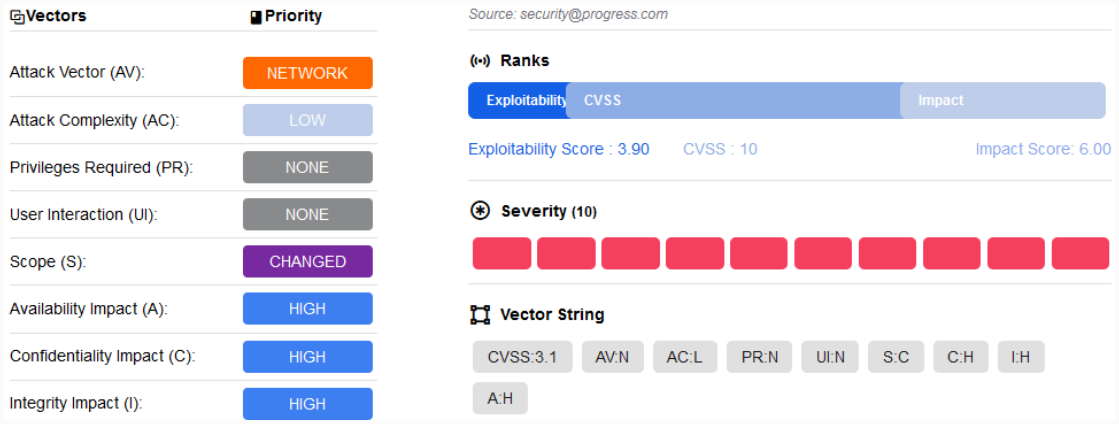


RelianceCyber

Improper Input Validation vulnerability in Progress LoadMaster

CVE ID	CVE-2024-7591
SUMMARY	Improper Input Validation vulnerability in Progress LoadMaster allows OS Command Injection. This issue affects:\n\n* LoadMaster: 7.2.40.0 and above\n\n* ECS: All versions\n\n* Multi-Tenancy: 7.1.35.4 and above
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	Apply updates.
VENDOR RECOMMENDATION	https://support.kemptechnologies.com/hc/en-us/articles/29196371689613-LoadMaster-Security-Vulnerability-CVE-2024-7591

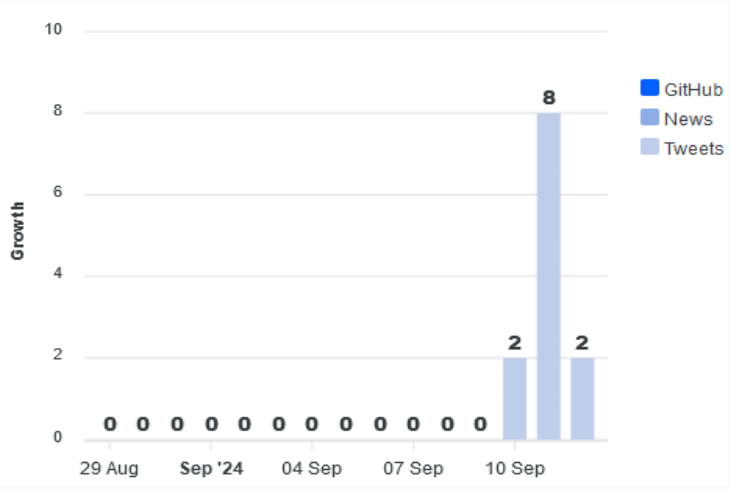


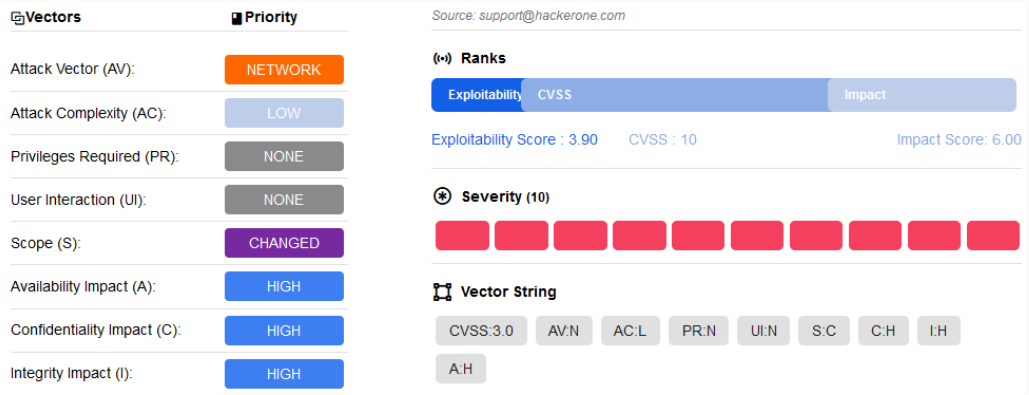


RelianceCyber

Deserialization of untrusted data in the agent portal of Ivanti EPM

CVE ID	CVE-2024-29847
SUMMARY	Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution.
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	Apply updates.
VENDOR RECOMMENDATION	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US

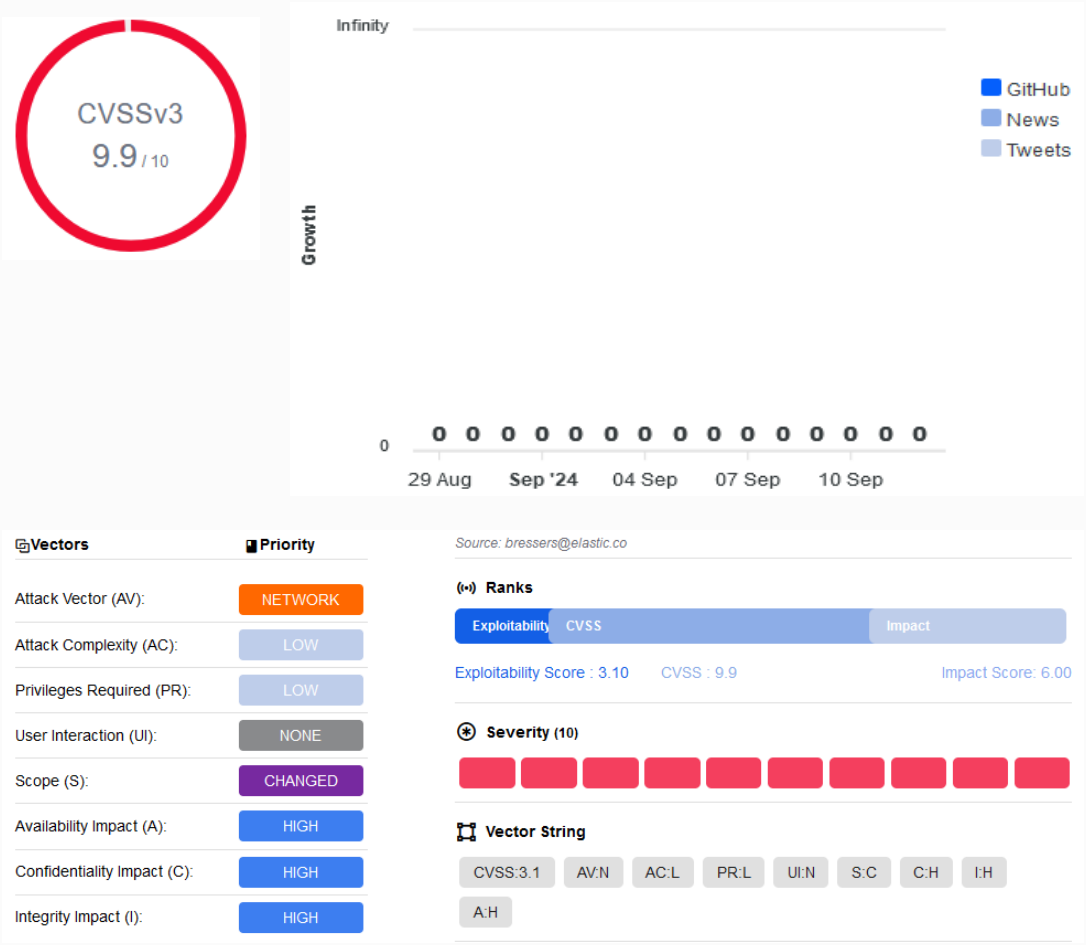




RelianceCyber

A deserialization issue in Kibana

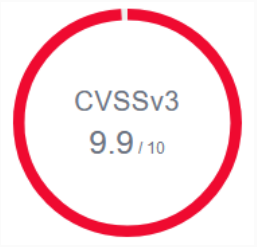
CVE ID	CVE-2024-37288
SUMMARY	A deserialization issue in Kibana can lead to arbitrary code execution when Kibana attempts to parse a YAML document containing a crafted payload. This issue only affects users that use Elastic Security's built-in AI tools https://www.elastic.co/guide/en/security/current/ai-for-security.html and have configured an Amazon Bedrock connector https://www.elastic.co/guide/en/security/current/assistant-connect-to-bedrock.html .
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Users should upgrade to version 8.15.1.
VENDOR RECOMMENDATION	https://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119

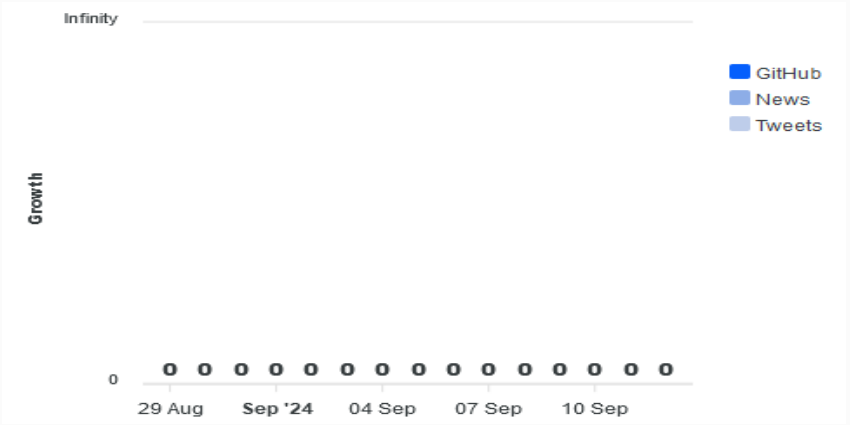


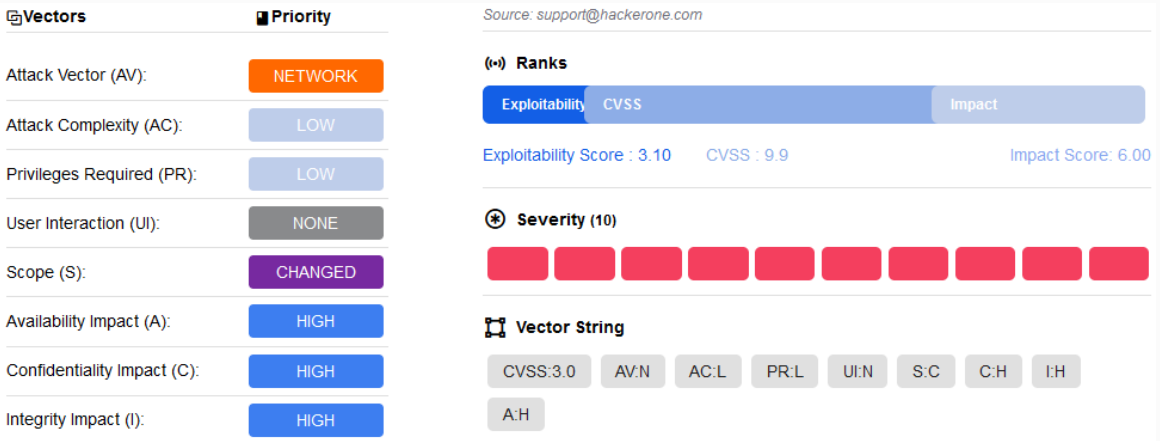
RelianceCyber

An authentication bypass vulnerability in Veeam VSPC Server

CVE ID	CVE-2024-38650
SUMMARY	An authentication bypass vulnerability can allow a low privileged attacker to access the NTLM hash of service account on the VSPC server.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Apply updates.
VENDOR RECOMMENDATION	https://www.veeam.com/kb4649



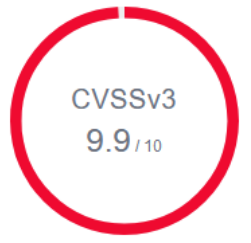


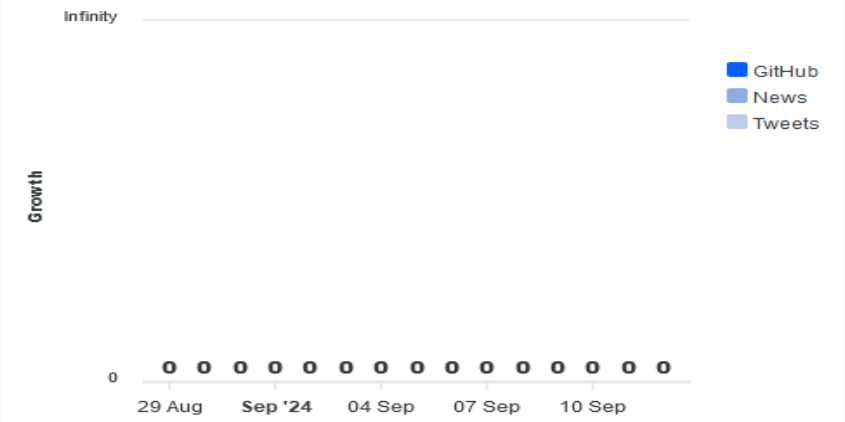


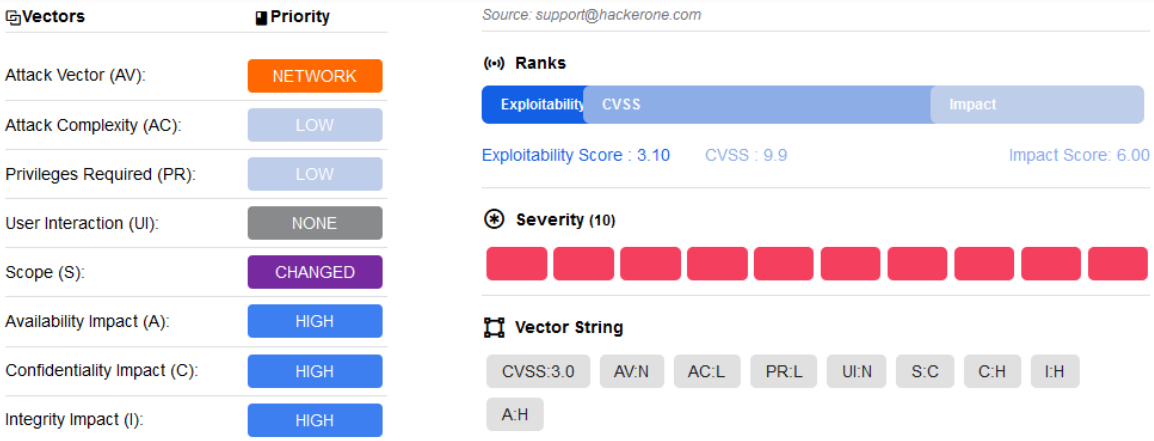
RelianceCyber

A code injection vulnerability in Veeam VSPC Server

CVE ID	CVE-2024-39714
SUMMARY	A code injection vulnerability that permits a low-privileged user to upload arbitrary files to the server, leading to remote code execution on VSPC server.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Apply updates.
VENDOR RECOMMENDATION	https://www.veeam.com/kb4649



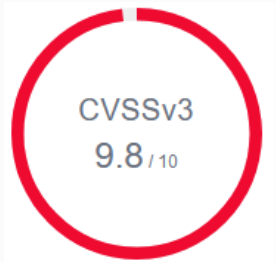


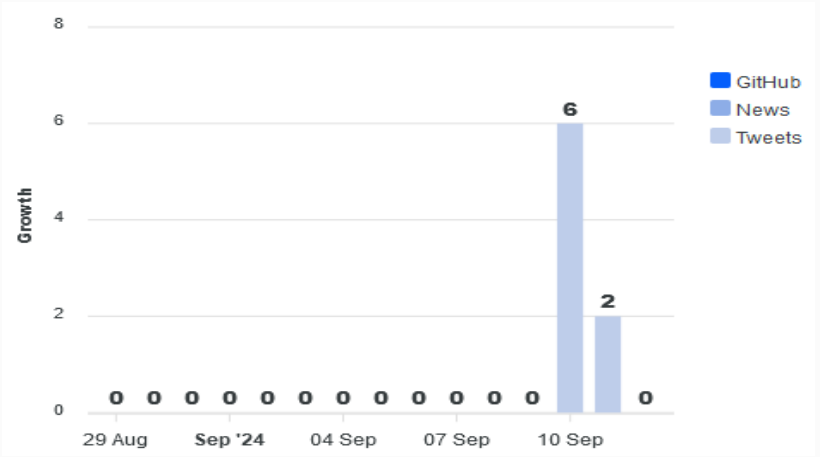


RelianceCyber

A command injection vulnerability in the export-cgi program of Zyxel NAS326

CVE ID	CVE-2024-6342
SUMMARY	**UNSUPPORTED WHEN ASSIGNED** A command injection vulnerability in the export-cgi program of Zyxel NAS326 firmware versions through V5.21(AAZF.18)C0 and NAS542 firmware versions through V5.21(ABAG.15)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Due to the critical severity of the vulnerability CVE-2024-6342, Zyxel has made hotfixes available to customers with extended support as outlined in the table below, despite the products already having reached end-of-vulnerability-support*.
VENDOR RECOMMENDATION	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-in-nas-products-09-10-2024





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)

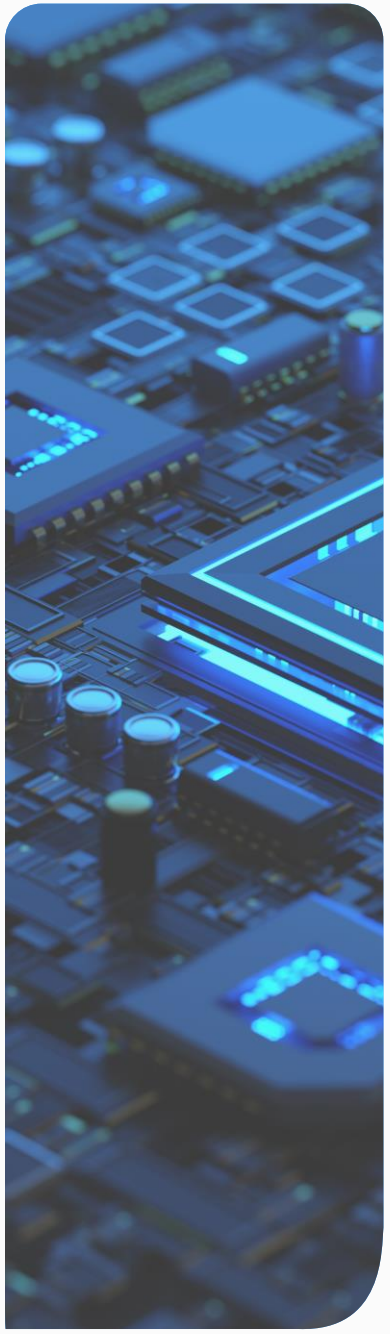
Vector String

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

RelianceCyber

TLP: CLEAR

Threat Intelligence



RelianceCyber

RansomHub Adopts New Techniques Using TDSSKiller and LaZagne Tools to Disable Security Defenses and Steal Credentials

RansomHub Ransomware Group is employing a new attack method that involves abusing legitimate tools, specifically TDSSKiller and LaZagne, as detailed in a ThreatDown report published on September 9, 2024. RansomHub deploys these tools following network reconnaissance and enumerating privileged accounts on target systems to disable security defenses and steal credentials from compromised networks. Notably, CISA did not include RansomHub's use of these tools in their advisory from August 29, 2024, indicating the group is constantly adopting new techniques beyond those previously reported. More details about the tools are outlined below:

TDSSKiller is a legitimate tool developed by Kaspersky to detect and remove rootkits and bootkits. RansomHub abused this tool to disable security protections such as Endpoint Detection and Response (EDR) systems. Specifically, RansomHub executes commands like 'tdsskiller.exe -dcsvc MBAMService' to disable security services, including Malwarebytes Anti-Malware Service (MBAMService), on compromised systems. Meanwhile, to evade detection, RansomHub runs TDSSKiller from a temporary directory with a dynamic filename.

LaZagne is a credential-harvesting tool that extracts login information from browsers, email clients, and databases. RansomHub deploys LaZagne after disabling MBAMService, to harvest this data. LaZagne also modifies files in the system and used that to store stolen credentials, and and deletes traces of infection to avoid detection. RansomHub then uses the stolen data, specifically database credentials, to escalate privileges, gain further access to sensitive data, and move laterally across the network.

RECOMMENDED ACTION

- Restrict Bring Your Own Vulnerable Driver (BYOVD) exploits: Implement controls to monitor and restrict vulnerable drivers like TDSSKiller, especially when executed with suspicious command-line flags such as -dcsvc. Quarantining or blocking known misuse patterns while allowing legitimate uses can prevent BYOVD attacks.

- Isolate critical systems: Use network segmentation to limit lateral movement. This can prevent attackers who gain access to credentials from spreading across the network and accessing sensitive databases.

SEE ALSO

https://www.threatdown.com/blog/new-ransomhub-attack-uses-tdskiller-and-lazagne-disables-edr/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

Insikt Group

RelianceCyber

CISA says SonicWall bug being exploited as experts warn of ransomware gang use

Federal cybersecurity experts are warning that a vulnerability affecting products from SonicWall is being exploited, and ordered all federal civilian agencies to implement a patch for the bug by the end of the month.

The Cybersecurity and Infrastructure Security Agency (CISA) said on Monday that hackers are exploiting CVE-2024-40766 — a vulnerability affecting SonicWall Gen 5 and Gen 6 devices, as well as Gen 7 devices running SonicOS 7.0.1-5035 and older versions.

SonicWall said in its own advisory that the vulnerability allows “unauthorized resource access” and in some situations can cause the firewall to crash. They have also confirmed that it is being exploited by hackers and said patches have been released.

For those unable to patch, SonicWall urged customers to ensure that access to the devices is limited or restricted from internet access. SonicWall gave the vulnerability a severity score of 9.3 out of 10.

The CISA warning comes days after researchers at Arctic Wolf said it observed hackers connected to the Akira ransomware gang exploiting the vulnerability.

CISA itself said it did not know if ransomware groups are exploiting the bug but Rapid7 confirmed on Monday that it has also seen ransomware actors exploiting it.

Arctic Wolf researchers saw affiliates of the group using compromised accounts on SonicWall devices as the initial access vector to carry out ransomware attacks.

“In each instance, the compromised accounts were local to the devices themselves rather than being integrated with a centralized authentication solution such as Microsoft Active Directory,” said Stefan Hostetler, senior threat intelligence researcher at Arctic Wolf.

RelianceCyber

“Additionally, [multifactor authentication] was disabled for all compromised accounts, and the SonicOS firmware on the affected devices were within the versions known to be vulnerable to CVE-2024-40766.”

Akira — responsible for attacks on Stanford University, cloud service Tietoevry and Yamaha — earned about $42 million in ransoms from attacks on at least 250 organizations since emerging in March 2023, according to the FBI.

The large number of attacks launched by the group led experts to believe it is made up of experienced actors and previous reports from Akira showed links between the gang and the now-defunct ransomware gang Conti.

RECOMMENDED ACTION

- SonicWall strongly advises that customers using GEN5 and GEN6 firewalls with SSLVPN users who have locally managed accounts immediately update their passwords to enhance security and prevent unauthorized access. Users can change their passwords if the "User must change password" option is enabled on their account. Administrators must manually enable the "User must change password" option for each local account to ensure this critical security measure is enforced.
- (GEN6 Firewalls) Additionally, SonicWall recommends enabling MFA (TOTP or Email-based OTP) for all SSLVPN users.

SEE ALSO

Insikt Group

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

RelianceCyber

Ivanti Patches Multiple Vulnerabilities in Endpoint Manager; No Active Exploitation Observed

On September 10, 2024, Ivanti addressed multiple vulnerabilities affecting its Endpoint Manager 2024 and 2022 SU5 versions. The Ivanti Endpoint Manager manages various IT assets, including desktops, laptops, and mobile devices. At the time of writing, there are no reports of these vulnerabilities being exploited in the wild.

Notable vulnerabilities patched include:

- **CVE-2024-37397**: Improperly sanitized XML inputs in the provisioning web service allow threat actors to access API secrets without authorization.
- **CVE-2024-8191**: Inadequate SQL input validation in the management console enables threat actors to perform unauthorized remote code execution.
- **CVE-2024-32840**, **CVE-2024-32841**, **CVE-2024-32842**, **CVE-2024-34783**, **CVE-2024-34784**, **CVE-2024-34785**: Threat actors with administrative privileges can execute remote code through a series of SQL injection vulnerabilities.
- **CVE-2024-8320** and **CVE-2024-8321**: Insufficient authentication measures in the network isolation features allow threat actors to tamper with networked devices' connectivity and security settings, likely leading to disruptions by isolating devices or falsely reporting their statuses.
- **CVE-2024-29847**: Unsafe deserialization practices in the agent portal allow threat actors to execute arbitrary code without authorization.

RelianceCyber

RECOMMENDED ACTION

Reliance Cyber recommends applying patches as per the vendor guidance.

SEE ALSO

Insikt Group

https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US

RelianceCyber

Volt Typhoon Exploits CVE-2024-39717, Deploys Custom Web Shell in Versa Director Servers to Access Networks

The Black Lotus Labs team discovered a zero-day exploit affecting Versa Director servers, as reported by SecurityWeek on August 26, 2024. The China-linked APT group Volt Typhoon exploited the vulnerability tracked as CVE-2024-39717 to deploy a custom-designed web shell on the servers called VersaMem.

This web shell enables the threat actors to intercept credentials and access networks of downstream customers such as Internet Service Providers (ISPs) and Managed Service Providers (MSPs). Versa Networks confirmed that threat actors compromised the crucial Versa Director GUI, which manages SD-WAN software, thus enabling unauthorized network access across multiple clients.

The threat actors gained initial administrative access via an exposed Versa management port (port 4566) intended for high-availability pairing of Director nodes, which creates redundancy within the SD-WAN managed by the Versa Director network nodes.

The VersaMem web shell hooks the setUserPassword method to intercept plaintext credentials. It also hooks the Catalina application filter chain to monitor all incoming traffic for actor-defined parameters, and dynamically loads malicious Java code exclusively in-memory. This in-memory manipulation leverages Java Instrumentation API and Javassist to alter Java classes in real-time, avoiding detection by traditional security measures. Versa Networks attributed this breach to a customer's failure to implement firewall guidelines issued in 2015 and 2017.

Volt Typhoon has conducted multiple campaigns targeting critical infrastructure and network devices in the US, Europe, and Asia since emerging around 2021. They frequently target both known and zero-day vulnerabilities in devices used by multiple organizations or infrastructure that enables them to access multiple networks.

RelianceCyber

Volt Typhoon does not usually deploy malware, but instead conducts hands-on-keyboard activity through command line or other custom web shells, relying on native programs to reduce their signature. However, they have developed custom malware and tools to exploit vulnerabilities tailored to the device or software, such as Impacket and Fast Reverse Proxy (FRP).

This is also not the first time Volt Typhoon has used compromised small office or home office (SOHO) devices as attack infrastructure. In February 2024, the US disrupted a botnet attributed to Volt Typhoon that used hundreds of compromised SOHO devices in the US to launch attacks against US Critical National Infrastructure. The targeting effort had been ongoing since at least 2022.

RECOMMENDED ACTION

Organizations managing Versa Director servers should immediately upgrade to version 22.1.4 (or later) or apply the hotfix described in Versa's security advisory sent to customers on August 8, 2024, and released to the public on August 26, 2024.

Defenders should also block and monitor external access to Port 4566 and Port 4570, ensuring these ports are only open between the active and standby Versa Director nodes for High-Availability-pairing traffic. Specific to Port 4566, Versa managers should search for and block interactions coming from non-Versa node IP addresses, such as those from SOHO networks.

Defenders should also scan the Windows directory and Versa webroot directory for abnormal files; this campaign used files with a .png extension.

However, these network artifacts could change as the tool evolves. Disabling or highly restricting privileges to alter the Windows directory and requiring active reauthorization before these alterations using multi-factor authentication (MFA) or other passwordless authentication can impede Volt Typhoon's ability to drop the malicious binaries and DLLs they use to execute their kill chains. Fileless malware that relies on LOLBins and in-memory execution techniques are often missed by traditional detection mechanisms. Defenders can conduct heuristic and behavioral analysis that examines command line execution for anomalous or out-of pattern activity.

SEE ALSO

Insikt Group

https://www.securityweek.com/chinese-apt-volt-typhoon-caught-exploiting-versa-networks-sd-wan-zero-day/

RELIANCECYBER.COM