RelianceCyber

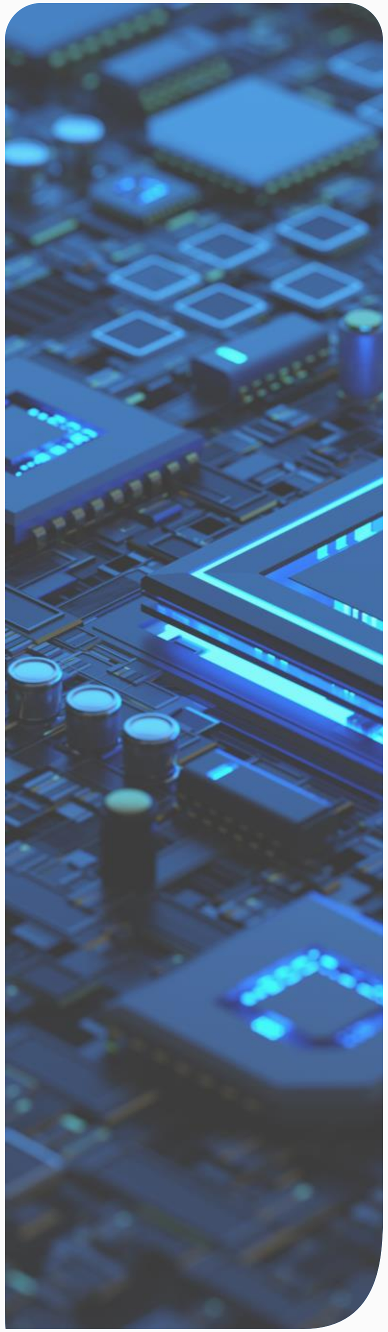
TLP: CLEAR

Threat Intelligence

WEEKLY BRIEFING

Written by: XDR Threat Intelligence Team

Date: 2024-10-03



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.

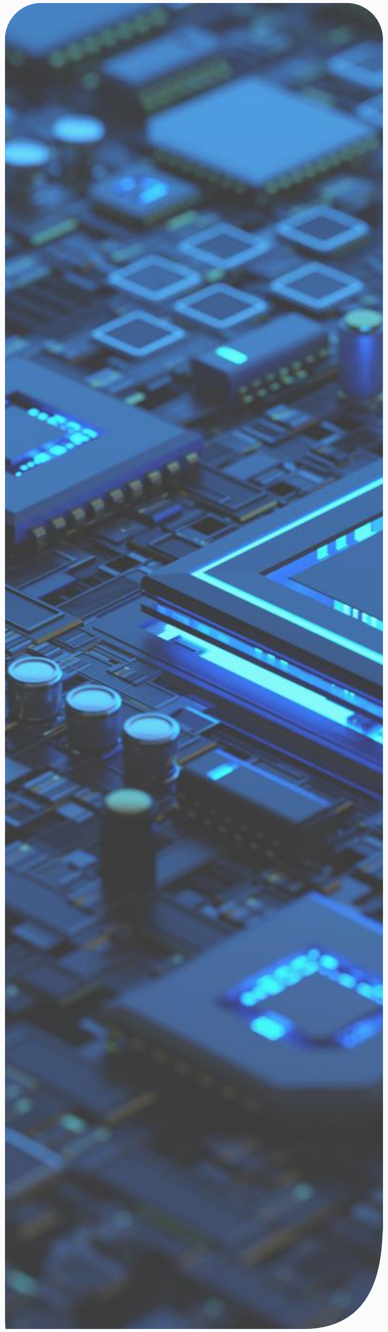
Please note that this information is based on the latest reports available and the situation may evolve.

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-2019-0344	SAP	Commerce	30/09/2024
CVE-2021-4043	Motion	Spell GPAC	30/09/2024
CVE-2020-15415	Draytek	Vigor Routers	30/09/2024
CVE-2023-25280	D-Link	DIR-820 Routers	30/09/2024
CVE-2024-29824	Ivanti	Endpoint Manager	02/10/2024

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
TeamViewer Remote Client	CVE-2024-7479, CVE-2024-7481	8.8	7
Nvidia Container Toolkit	CVE-2024-0132	8.3	8
Cisco Nexus Dashboard Fabric Controller (NDFC)	CVE-2024-20432, CVE-2024-20449	8.8-9.9	9
Zimbra Collaboration	CVE-2024-45519	9.8	10
Cisco Small Business Routers	CVE-2024-20393	8.8	11

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

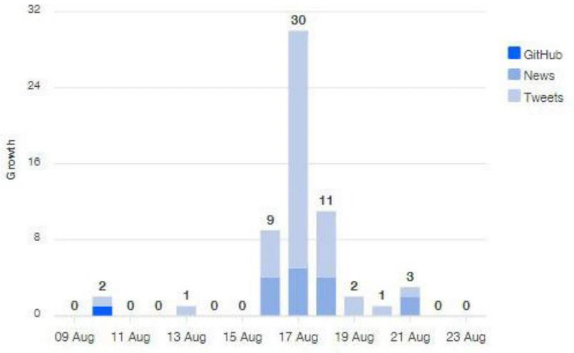
BASE METRIC CATEGORY	DESCRIPTION	OPTION
Attack Vector (AV)	This metric reflects the context by which vulnerability exploitation is possible.	Network Adjacent. Local, Physical
Attack Complexity (AC)	This metric describes the conditions beyond the attacker's control that must exist in order to exploit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

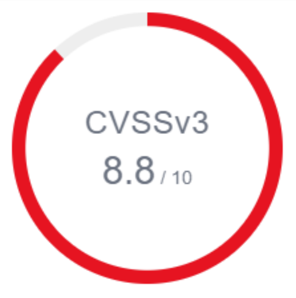
For more details about the CVSS Metrics, please see this resource: https://www.first.org/cvss/v3.1/specification-document



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

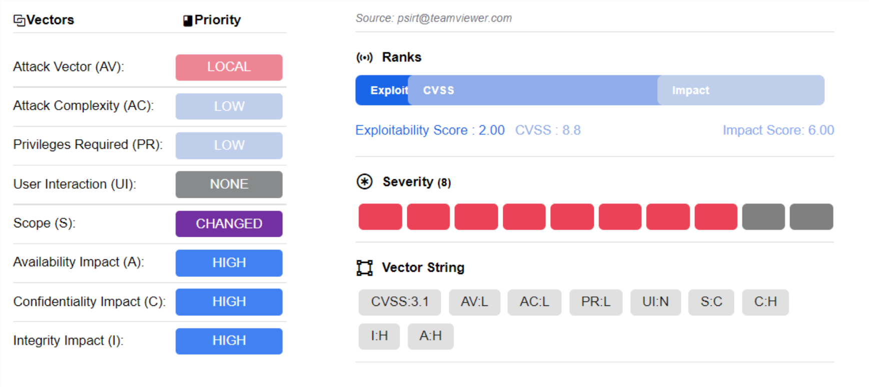
Elevation Privilege Vulnerability in TeamViewer Remote Client

CVE ID	CVE-2024-7479, CVE-2024-7481
SUMMARY	Improper verification of cryptographic signature during installation of a VPN and Printer drivers via the TeamViewer_service.exe component of TeamViewer Remote Clients prior version 15.58.4 for Windows allows an attacker with local unprivileged access on a Windows system to elevate their privileges and install drivers.
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2024-1006/



CVSSv3

8.8 / 10



Vectors	Priority
Attack Vector (AV):	LOCAL
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@teamviewer.com

Ranks

Exploit CVSS Impact

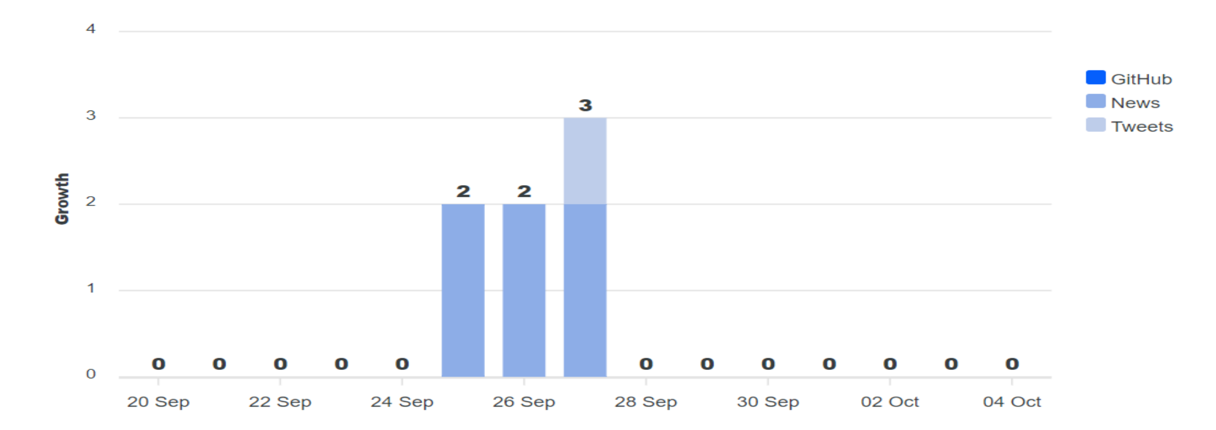
Exploitability Score : 2.00 CVSS : 8.8 Impact Score: 6.00

Severity (8)

🟥🟥🟥🟥🟥🟥🟥🟥⬛⬛

Vector String

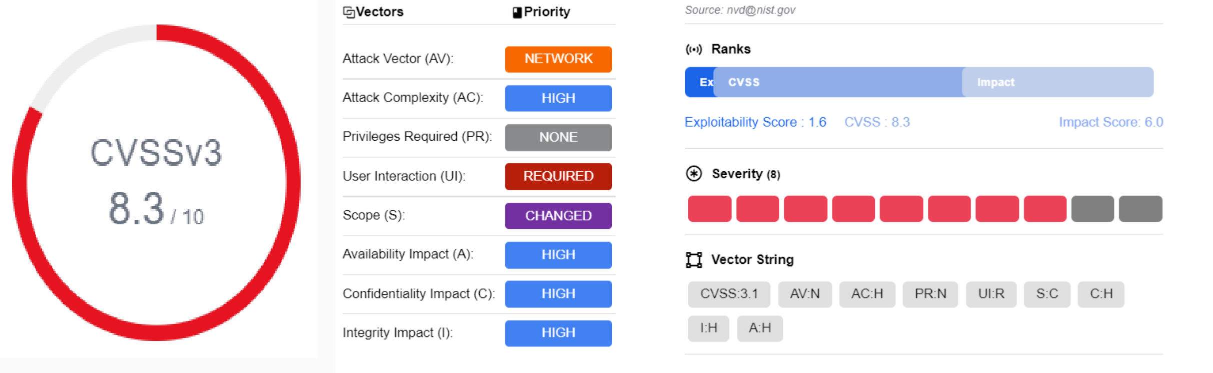
CVSS:3.1 AV:L AC:L PR:L UI:N S:C C:H I:H A:H



RelianceCyber

Nvidia Container Toolkit Time-of-check Time-of-Use Vulnerability

CVE ID	CVE-2024-0132
SUMMARY	NVIDIA Container Toolkit 1.16.1 or earlier contains a Time-of-check Time-of-Use (TOCTOU) vulnerability when used with default configuration where a specifically crafted container image may gain access to the host file system. This does not impact use cases where CDI is used. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.
EXPLOITED IN THE WILD	No
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://nvidia.custhelp.com/app/answers/detail/a_id/5582
SEE ALSO	https://www.wiz.io/blog/wiz-research-critical-nvidia-ai-vulnerability



CVSSv3 8.3 / 10

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

Source: nvd@nist.gov

Ranks

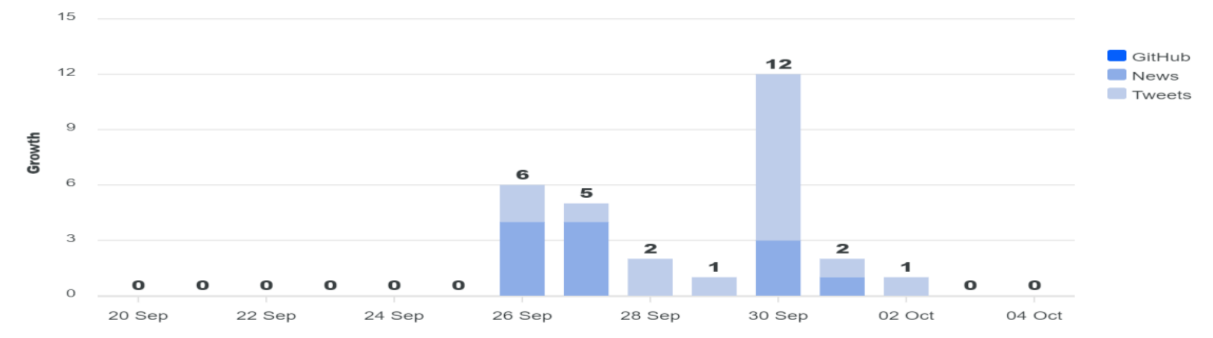
Exploitability Score : 1.6 CVSS : 8.3 Impact Score: 6.0

Severity (8)

🟥🟥🟥🟥🟥🟥🟥🟥⬛⬛

Vector String

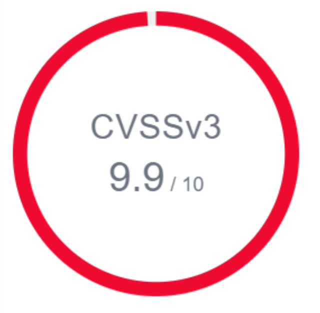
CVSS:3.1 AV:N AC:H PR:N UI:R S:C C:H I:H A:H

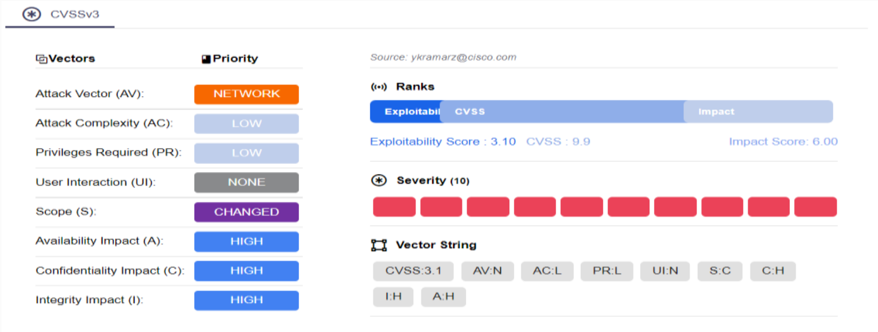


RelianceCyber

Remote Code and Command Injection Vulnerabilities in Cisco Nexus Dashboard Fabric Controller (NDFC)

CVE ID	CVE-2024-20432, CVE-2024-20449
SUMMARY	Vulnerabilities in Cisco Nexus Dashboard Fabric Controller (NDFC) allowing a remote attacker to perform command and arbitrary code injections on an affected device.
EXPLOITED IN THE WILD	No
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-ptrce-BUSHLbp





CVSSv3

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: ykramarz@cisco.com

Ranks

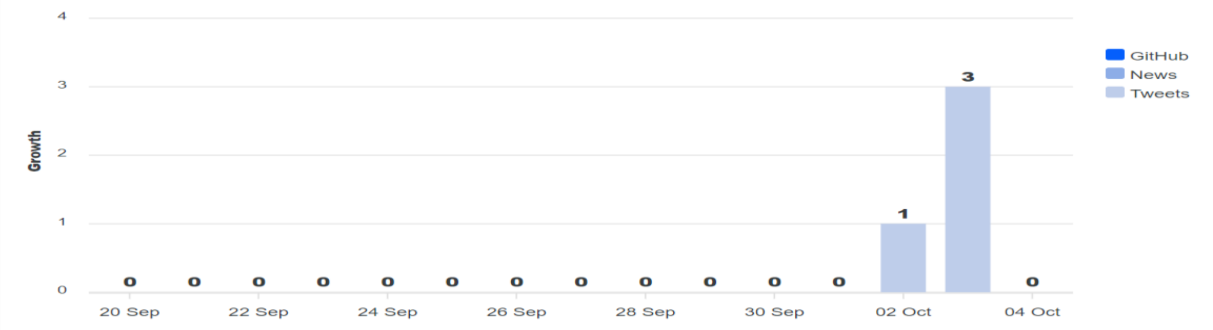
Exploitabil CVSS Impact

Exploitability Score : 3.10 CVSS : 9.9 Impact Score: 6.00

Severity (10)

Vector String

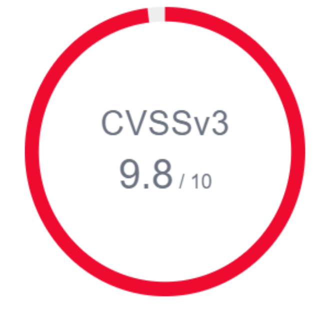
CVSS:3.1 AV:N AC:L PR:L UI:N S:C C:H I:H A:H

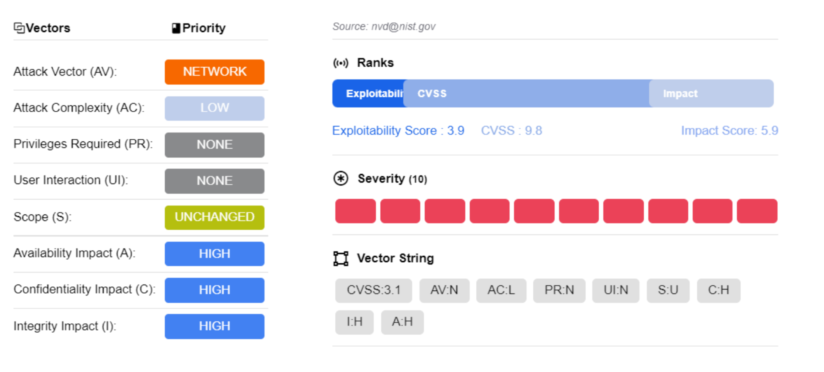


RelianceCyber

Unauthenticated command execution vulnerability in Zimbra Collaboration

CVE ID	CVE-2024-45519
SUMMARY	The postjournal service in Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 sometimes allows unauthenticated users to execute commands.
EXPLOITED IN THE WILD	Yes (Exploit Publicly Available)
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://wiki.zimbra.com/wiki/Security_Center
SEE ALSO	https://blog.projectdiscovery.io/zimbra-remote-code-execution/





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

Exploitabili CVSS Impact

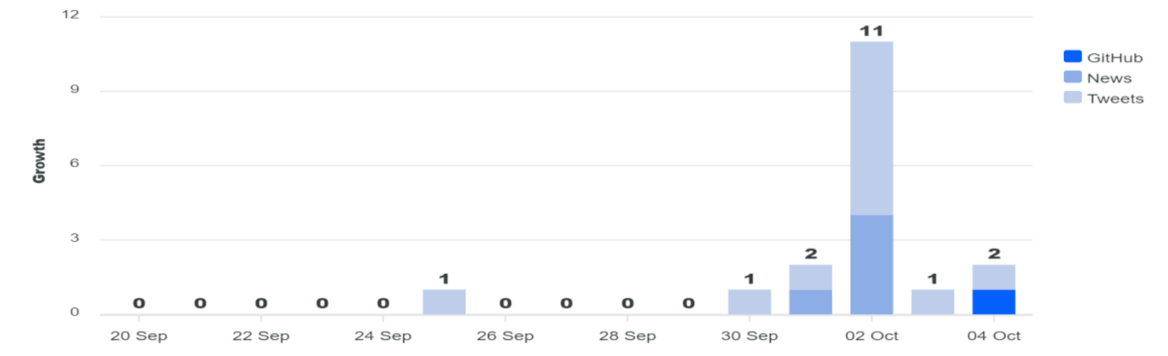
Exploitability Score : 3.9 CVSS : 9.8 Impact Score: 5.9

Severity (10)

🟥🟥🟥🟥🟥🟥🟥🟥🟥🟥

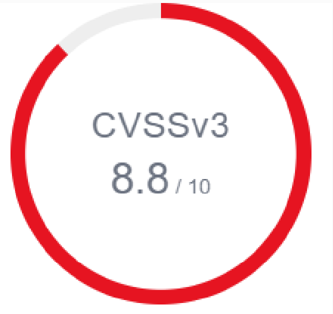
Vector String

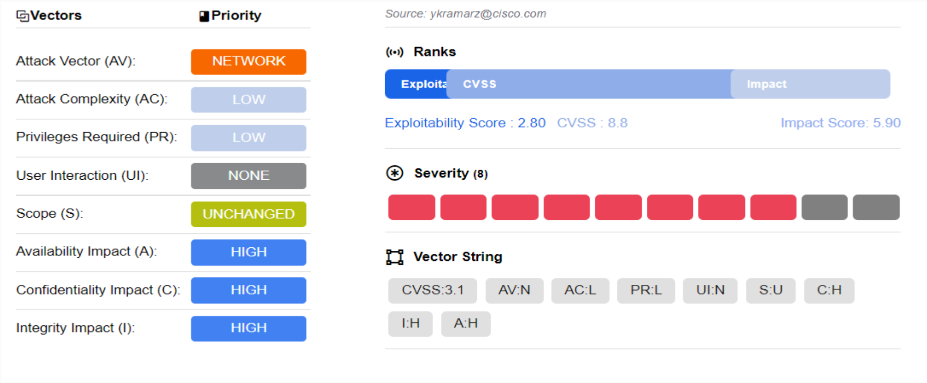
CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H A:H



Privilege Escalation Vulnerability in Cisco Small Business Routers

CVE ID	CVE-2024-20393
SUMMARY	A vulnerability in the web-based management interface of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability exists because the web-based management interface discloses sensitive information. An attacker could exploit this vulnerability by sending crafted HTTP input to an affected device. A successful exploit could allow an attacker to elevate privileges from guest to admin.
EXPLOITED IN THE WILD	No
VENDOR SUGGESTED ACTION	Vendor has advised that no patch or workaround is available or will be provided, due to products being past their end of software maintenance releases.
VENDOR RECOMMENDATION	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms





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

Source: ykramarz@cisco.com

Ranks

Exploita CVSS Impact

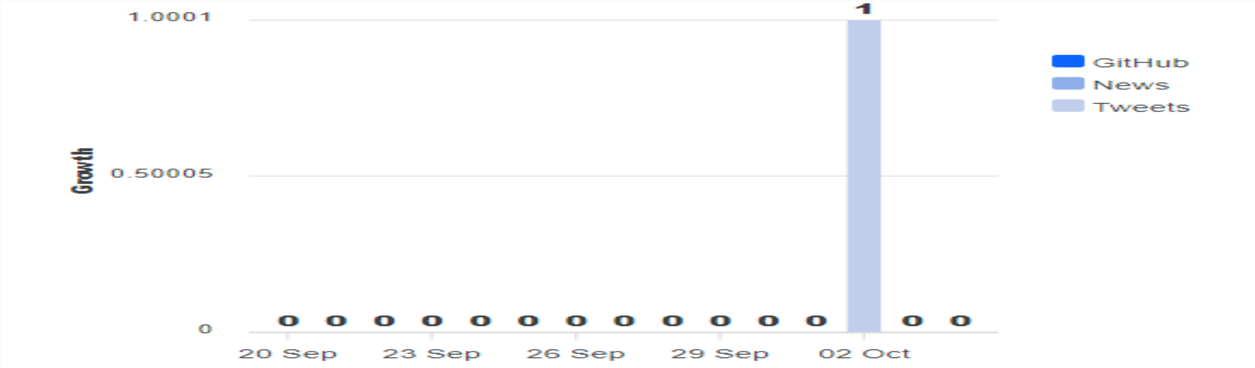
Exploitability Score : 2.80 CVSS : 8.8 Impact Score: 5.90

Severity (8)

🟥 🟥 🟥 🟥 🟥 🟥 🟥 🟥 ⬛ ⬛

Vector String

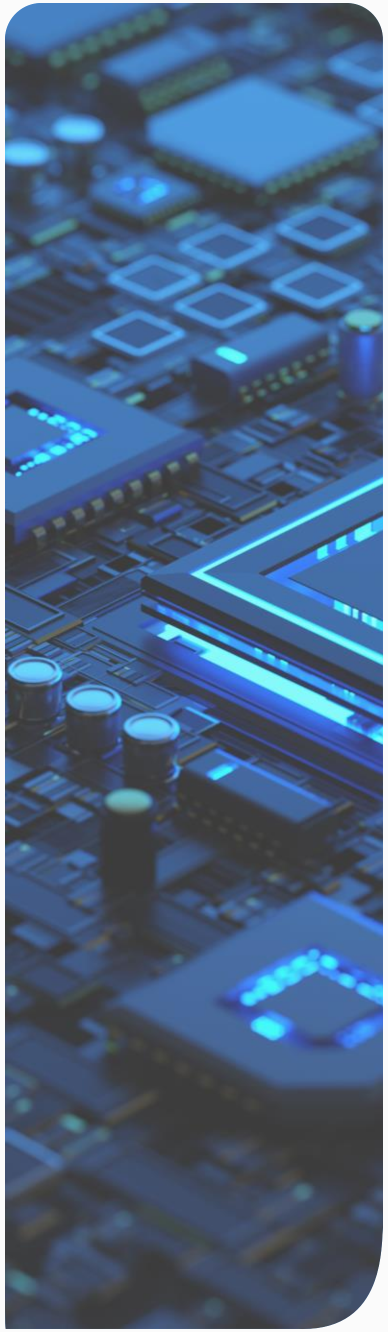
CVSS:3.1 AV:N AC:L PR:L UI:N S:U C:H I:H A:H



RelianceCyber

TLP: CLEAR

Threat Intelligence



RelianceCyber

Irish Data Protection Commission fines Meta Ireland €91 million

The Data Protection Commission (DPC) has today announced its final decision following an inquiry into Meta Platforms Ireland Limited (MPIL). This inquiry was launched in April 2019, after MPIL notified the DPC that it had inadvertently stored certain passwords of social media users in 'plaintext' on its internal systems (i.e. without cryptographic protection or encryption).

RECOMMENDED ACTION

Companies should ensure that they are storing any customer data in a secure manner.

SEE ALSO

https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-91-million-fine-of-Meta

RelianceCyber

700K+ DrayTek routers are sitting ducks on the internet, open to remote hijacking

Forescout Research have discovered 14 new vulnerabilities in DrayTek Vigor routers. In combination to this, currently over 700000 DrayTek routers are accessible on the internet via their control panels, meaning that if these 14 new vulnerabilities go unpatched they are likely to be heavily exploited. Of the 14 vulnerabilities, one is a 10 CVSS remote code execution flaw.

Just last month, the FBI reported on Chinese backed Threat Actors had exploited 3 existing CVE's in Draytek Routers as part of creating a 250000 device Botnet.

RECOMMENDED ACTION

Companies using DrayTek routers should ensure that all vulnerabilities are patched, and that control panels are not accessible to the internet.

SEE ALSO

https://www.forescout.com/resources/draybreak-draytek-research/
https://www.theregister.com/2024/10/02/draytek_routers_bugs/

RelianceCyber

Ongoing Threat of Spear-Phishing Attacks carried out by Iranian backed Threat Actors

In an advisory published with US partners, the National Cyber Security Centre – a part of GCHQ – has shared technical details about how cyber attackers working on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC) are using social engineering techniques to gain access to victims' personal and business accounts online.

The malicious activity is targeted against individuals with a nexus to Iranian and Middle Eastern affairs, such as current and former senior government officials, senior think tank personnel, journalists, activists and lobbyists. The US has also observed targeting of persons associated with US political campaigns.

RECOMMENDED ACTION

Individuals as described above who are at higher risk should stay vigilant and follow the applicable advice [from the NCSC.](https://www.ncsc.gov.uk)

SEE ALSO

https://www.ncsc.gov.uk/news/uk-us-issue-alert-cyber-actors-behalf-iranian-state-carry-targeted-phishing-attacks

https://www.ic3.gov/Media/News/2024/240927.pdf

North Korea Hackers Linked to Breach of German Missile Manufacturer

Kimusky (APT-43) are reported to have breached Diehl Defence, a German company that manufactures Iris-T air defense systems, using a clever phishing campaign with fake job offers and advanced social engineering tactics, according to a report by Der Spiegel.

The attack combined the use of booby-trapped PDF files with spear-phishing lures offering Diehl Defence employees jobs with American defence contractors.

The targeting of Diehl Defence is significant because the company specializes in the production of missiles and ammunition. Last October, Diehl Defence inked a deal to supply South Korea with its Iris-T short-range air-to-air missiles.

RECOMMENDED ACTION

Companies should provide employees with regular awareness training around social engineering.

In addition to this, Phishing Simulation training should also be carried out for all users, so they understand these threats and what they need to be aware of.

SEE ALSO

https://www.securityweek.com/north-korea-hackers-linked-to-breach-of-german-missile-manufacturer/

https://www.spiegel.de/netzwelt/web/diehl-defence-hacker-aus-nordkorea-zielen-auf-mitarbeiter-des-ruestungskonzerns-a-8735f440-670c-40df-9e46-06c620fe9be6

RelianceCyber

Rackspace monitoring data stolen in ScienceLogic zero-day attack

Cloud hosting provider Rackspace suffered a data breach exposing "limited" customer monitoring data after threat actors exploited a zero-day vulnerability in a third-party tool used by the ScienceLogic SL1 platform. ScienceLogic confirmed to BleepingComputer that they quickly developed a patch to address the risk and distributed it to all impacted customers while still providing assistance where needed.

"We identified a zero-day remote code execution vulnerability within a non-ScienceLogic third-party utility that is delivered with the SL1 package," explained a statement from Jessica Lindberg, Vice President at ScienceLogic. "Upon identification, we rapidly developed a patch to remediate the incident and have made it available to all customers globally.“

In an email sent to customers and seen by The Register, Rackspace warned that the hackers exploited the zero-day to gain access to web servers and steal limited customer monitoring data, including customer account names and numbers, customer usernames, Rackspace internally generated device IDs, device name and information, IP addresses, and AES256 encrypted Rackspace internal device agent credentials. Rackspace rotated those credentials as a precaution, despite them being strongly encrypted, and informed customers they needed to take no further action to protect from the malicious activity, which had been stopped.

RECOMMENDED ACTION

Companies using Rackspace should have been contacted directly by the vendor, however no actions appear to be required.

SEE ALSO

https://www.bleepingcomputer.com/news/security/rackspace-monitoring-data-stolen-in-sciencelogic-zero-day-attack/

RelianceCyber

RELIANCECYBER.COM