RelianceCyber

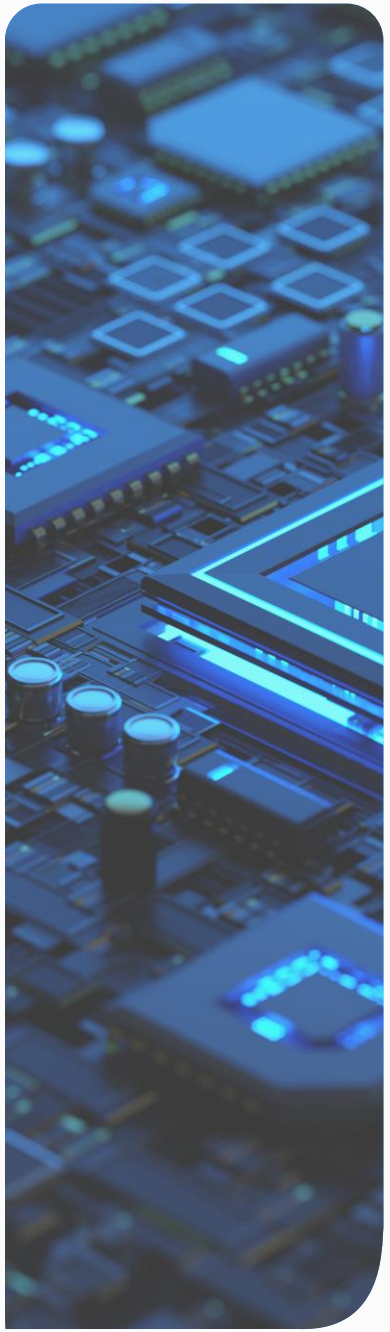
TLP: CLEAR

Threat Intelligence

WEEKLY BRIEFING

Written by: XDR Threat Intelligence Team

Date: 2024-09-19



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.

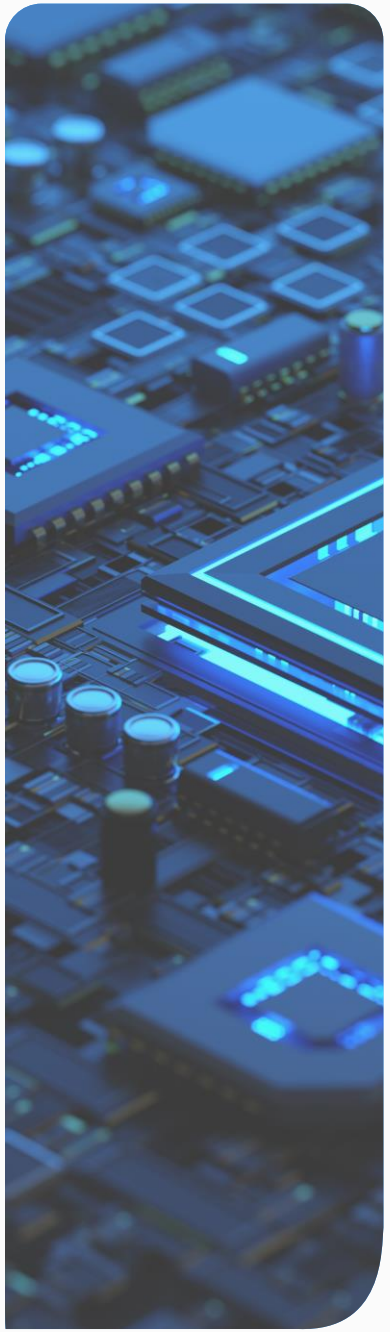
In all cases, Reliance Cyber recommends that, where possible, you closely follow the manufacturer's latest advice to mitigate any vulnerabilities.

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-2024-8190	Ivanti	Cloud Services Appliance	16/09/2024
CVE-2024-6670	Progress	WhastsUp Gold	16/09/2024
CVE-2024-43461	Microsoft	Windows	16/09/2024
CVE-2014-0502, CVE-2013-0643, CVE-2014-0497	Adobe	Flash Player	17/09/2024
CVE-2020-14644	Oracle	WebLogic Server	18/09/2024
CVE-2022-21445	Oracle	JDeveloper	18/09/2024
CVE-2019-1069	Microsoft	Windows	18/09/2024
CVE-2020-0618	Microsoft	Windows	18/09/2024
CVE-2024-27348	Apache	HugeGraph-Server	18/09/2024

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
Ivanti EPM	CVE-2024-29847, CVE-2024-32840, CVE-2024-32842, CVE-2024-32845,CVE-2024-32846,CVE-2024-32848, CVE-2024-34779, CVE-2024-34783, CVE-2024-34785	9.1-10	7
SolarWinds ARM	CVE-2024-28990, CVE-2024-28991	9.0-9.8	8
Docker Desktop	CVE-2024-8695, CVE-2024-8696	9.0-9.8	9
Gitlab Community and Enterprise	CVE-2024-6678	8.8	10
Vmware vCenter	CVE-2024-38812	9.8	11
Google Chrome	CVE-2024-8905, CVE-2024-8906	8.8	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

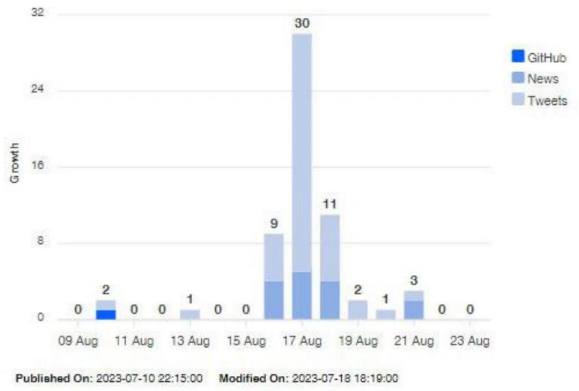
BASE METRIC CATEGORY	DESCRIPTION	OPTION
Attack Vector (AV)	This metric reflects the context by which vulnerability exploitation is possible.	Network Adjacent. Local, Physical
Attack Complexity (AC)	This metric describes the conditions beyond the attacker's control that must exist in order to exploit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

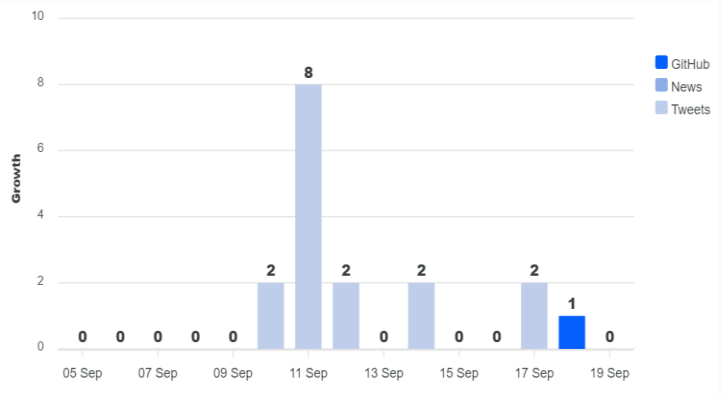
For more details about the CVSS Metrics, please see this resource: https://www.first.org/cvss/v3.1/specification-document

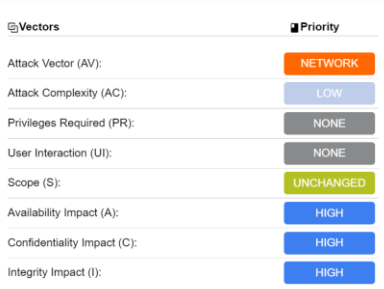


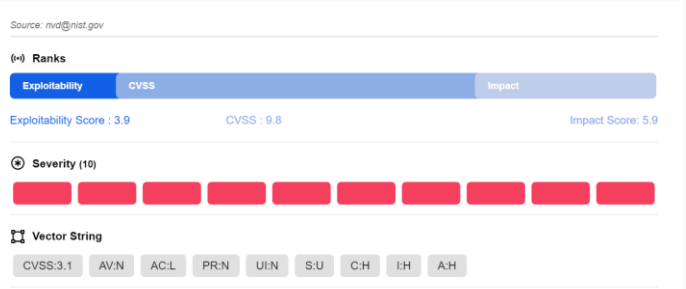
RelianceCyber

Ivanti Endpoint Manager - Various Vulnerabilities

CVE ID	CVE-2024-29847, CVE-2024-32840, CVE-2024-32842, CVE-2024-32845,CVE-2024-32846,CVE-2024-32848, CVE-2024-34779, CVE-2024-34783, CVE-2024-34785
SUMMARY	Various vulnerabilities have been reported in Ivanti Endpoint Manager.
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022?language=en_US



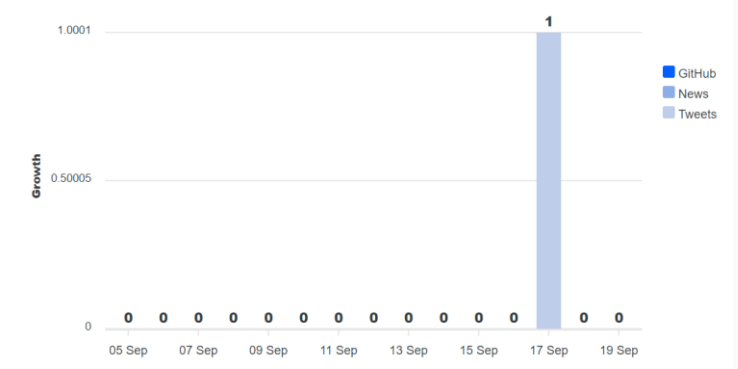


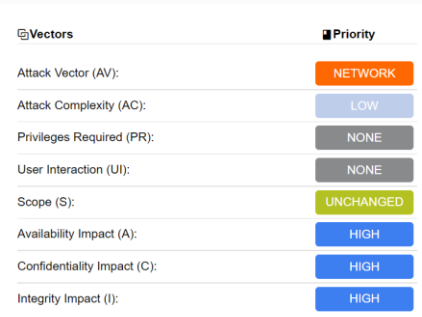


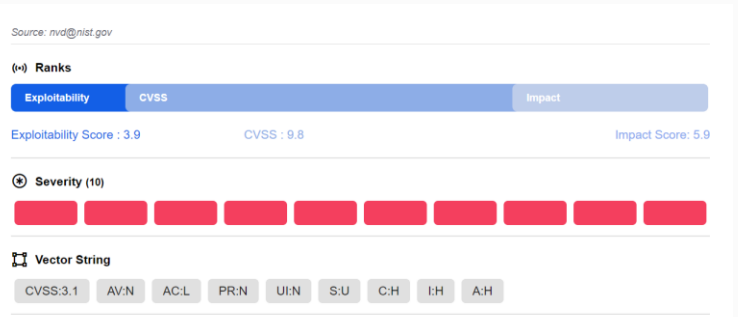
RelianceCyber

SolarWinds Access Rights Manager – Remote Code Execution and Hard Coded Credential Bypass

CVE ID	CVE-2024-28990, CVE-2024-28991
SUMMARY	Remote Code Execution and Hard Coded Credential Bypass in SolarWinds Access Rights Manager (ARM)
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28990 / https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28991



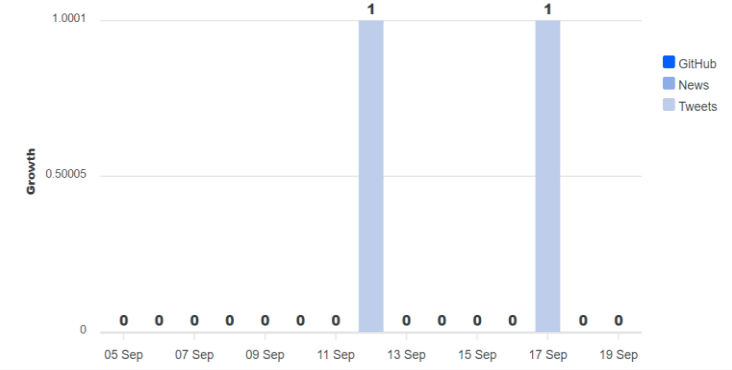


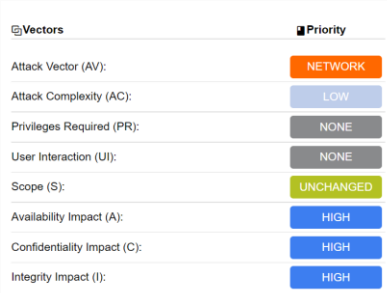


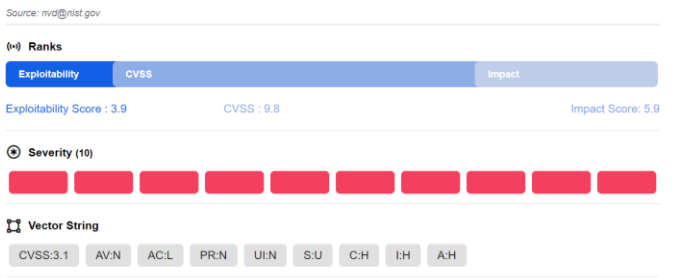
RelianceCyber

Docker Desktop – Remote Code Execution

CVE ID	CVE-2024-8695, CVE-2024-8696
SUMMARY	Remote Code Execution in Docker Desktop
EXPLOITED IN THE WILD	No
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://docs.docker.com/desktop/release-notes/#4342



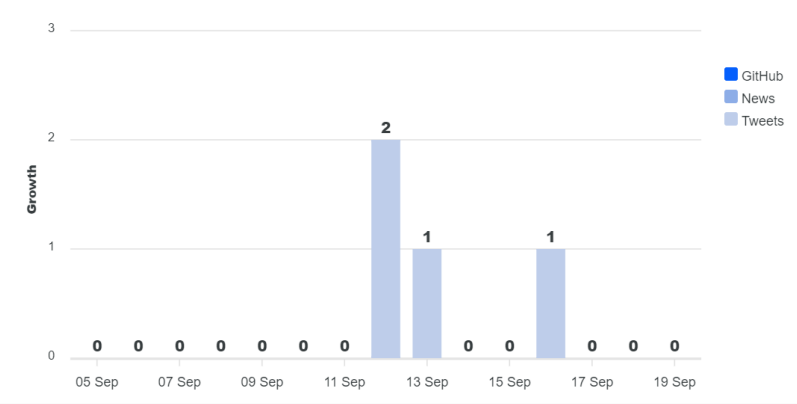


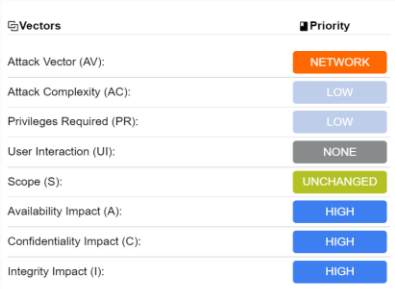


RelianceCyber

GitLab Community and Enterprise – Pipeline Trigger as an Arbitrary User

CVE ID	CVE-2024-6678
SUMMARY	An issue was discovered in GitLab CE/EE affecting all versions starting from 8.14 prior to 17.1.7, starting from 17.2 prior to 17.2.5, and starting from 17.3 prior to 17.3.2, which allows an attacker to trigger a pipeline as an arbitrary user under certain circumstances.
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://about.gitlab.com/releases/2024/09/11/patch-release-gitlab-17-3-2-released/

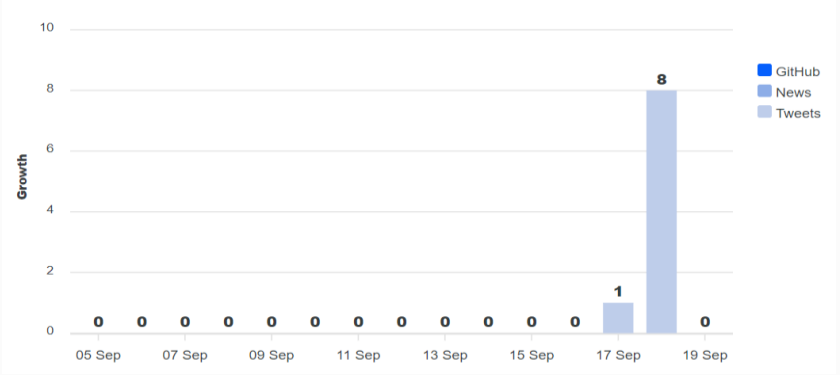


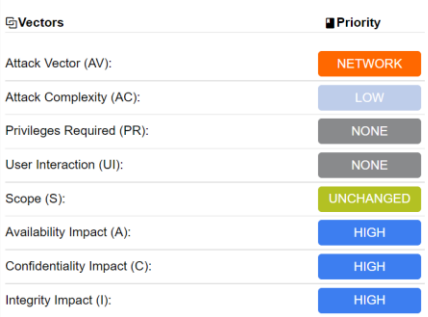


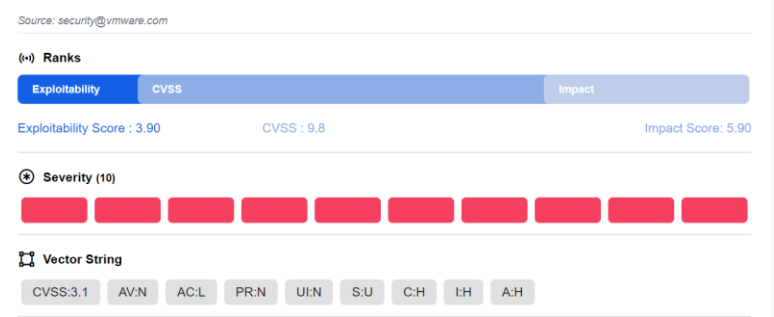
RelianceCyber

Vmware vCenter - Heap Overflow Vulnerability

CVE ID	CVE-2024-38812
SUMMARY	The vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.
EXPLOITED IN THE WILD	No
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968



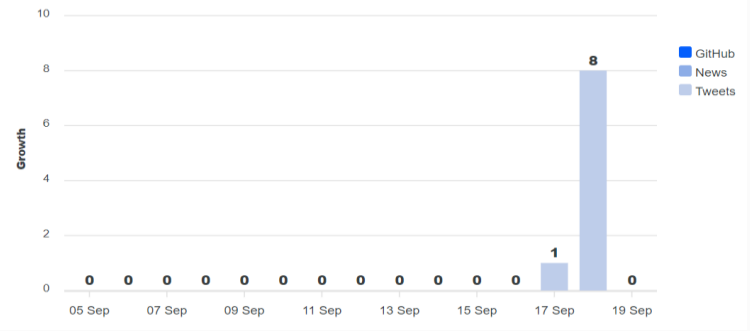


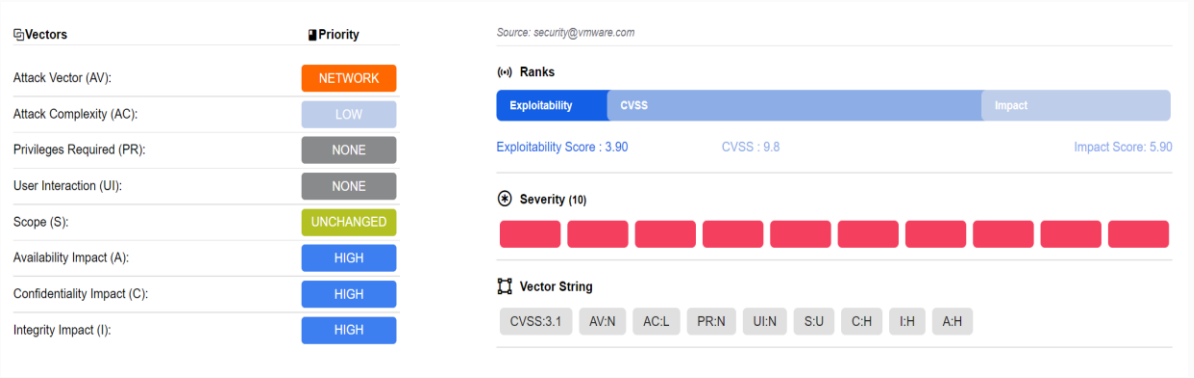


RelianceCyber

Google Chrome – Exploit Stack and Heap Corruption Vulnerabilities

CVE ID	CVE-2024-8905, CVE-2024-8906
SUMMARY	A remote attacker was potentially able to exploit stack corruption and heap corruption via a crafted HTML page.
EXPLOITED IN THE WILD	Yes
VENDOR SUGGESTED ACTION	Patch
VENDOR RECOMMENDATION	https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_17.html

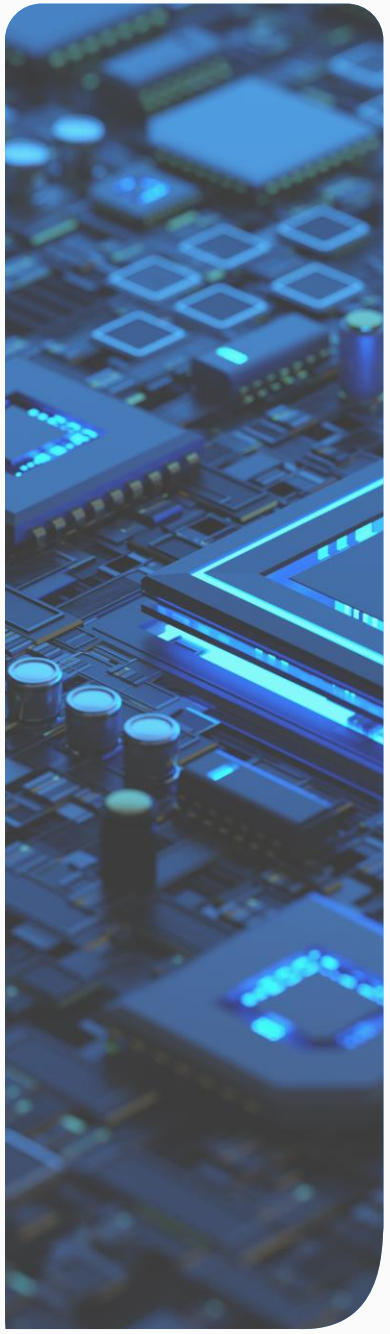




RelianceCyber

TLP: CLEAR

Threat Intelligence



RelianceCyber

People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations

The NCSC along with partners has reported that the People's Republic of China (PRC)-linked cyber actors have compromised thousands of Internet-connected devices, including small office/home office (SOHO) routers, firewalls, network-attached storage (NAS) and Internet of Things (IoT) devices with the goal of creating a network of compromised nodes (a "botnet") positioned for malicious activity. The actors may then use the botnet as a proxy to conceal their identities while deploying distributed denial of service (DDoS) attacks or compromising networks.

Integrity Technology Group, a PRC-based company, has controlled and managed a botnet active since mid 2021. The botnet has regularly maintained between tens to hundreds of thousands of compromised devices.

As of June 2024, the botnet consisted of over 260,000 devices. Victim devices part of the botnet have been observed in North America, South America, Europe, Africa, Southeast Asia and Australia. While devices aged beyond their end-of-life dates are known to be more vulnerable to intrusion, many of the compromised devices in the Integrity Tech controlled botnet are likely still supported by their respective vendors.

RECOMMENDED ACTION

- Reliance Cyber recommends following the steps outlined in the "Recommended Mitigations" section of the article.
- All IOCs outlined within the article have been checked on Reliance Cyber XDR customer networks already. If you are not a Reliance Cyber XDR customer, we recommend doing this.

RelianceCyber

Enterprise ServiceNow Knowledge Bases at Risk : Extensive Data Exposures Uncovered

Researchers at AppOmni have discovered that over a thousand ServiceNow online instances are unintentionally exposing company information due to configuration issues with Knowledge Bases.

The exposed information includes personally identifiable information (PII), internal system details, user credentials, access tokens for live production systems, and other essential information depending on the Knowledge Base topic.

To note - Reliance Cyber have already confirmed that we are not impacted by this configuration issue, however we urge all customers using ServiceNow to follow the below recommendations; and to pass this advice onto any 3rd parties who may also be impacted.

RECOMMENDED ACTION

- Reliance Cyber recommends following the "How to Mitigate ServiceNow KB Data Risks" section of the AppOmni article.

RelianceCyber

CISA warns of Windows flaw used in infostealer malware attacks

CISA has ordered U.S. federal agencies to secure their systems against a recently patched Windows MSHTML spoofing zero-day bug exploited by the Void Banshee APT hacking group.

The vulnerability (CVE-2024-43461) was disclosed during this month's Patch Tuesday, and Microsoft initially classified it as not exploited in attacks. However, Microsoft updated the advisory on Friday to confirm that it had been exploited in attacks before being fixed.

Microsoft revealed that attackers exploited CVE-2024-43461 before July 2024 as a part of an exploit chain with CVE-2024-38112, another MSHTML spoofing bug.

"We released a fix for CVE-2024-38112 in our July 2024 security updates which broke this attack chain," it said. "Customers should both the July 2024 and September 2024 security update to fully protect themselves."

RECOMMENDED ACTION

- Reliance Cyber recommends ensuring you have applied that July and September 2024 Windows Security Updates as per the Microsoft advice outlined above.

RelianceCyber

Clever 'GitHub Scanner' campaign abusing repos to push malware

A threat campaign is abusing GitHub repositories to distribute the Lumma Stealer password-stealing malware targeting users who frequent an open source project repository or are subscribed to email notifications from it.

A malicious GitHub user opens a new "issue" on an open source repository falsely claiming that the project contains a "security vulnerability" and urges others to visit a counterfeit "GitHub Scanner" domain. The domain in question, however, is not associated with GitHub and tricks users into installing Windows malware.

GitHub users have been receiving email notifications this week urging them to address a bogus "security vulnerability" in a project repo that they have contributed to, or are otherwise subscribed to.

Users are advised to visit "github-scanner[.]com" to learn more about the alleged security issue.

To make the lure more convincing, the email originates from legitimate GitHub email address, notifications@github.com, and is signed "Best regards, Github Security Team" in the message body.

RECOMMENDED ACTION

- Reliance Cyber recommends blocking the above domain on all suitable controls.
- Reliance Cyber XDR customers have had this domain checked for them on their networks already.

RelianceCyber

Hadooken Malware Targets Weblogic Applications

Researchers from Aqua Security have discovered that hackers are targeting Oracle WebLogic servers to infect them with a new Linux malware named "Hadooken," which launches a cryptominer and a tool for distributed denial-of-service (DDoS) attacks. The access obtained may also be used to execute ransomware attacks on Windows systems.

An attack was observed on a honeypot, which the threat actor breached due to weak credentials.

Based on the researchers' findings using the Shodan search engine for internet-connected devices, there are more than 230,000 Weblogic servers on the public web.

RECOMMENDED ACTION

- Reliance Cyber recommends following the mitigation advice stated within the AquaSec advisory.

RELIANCECYBER.COM