

---

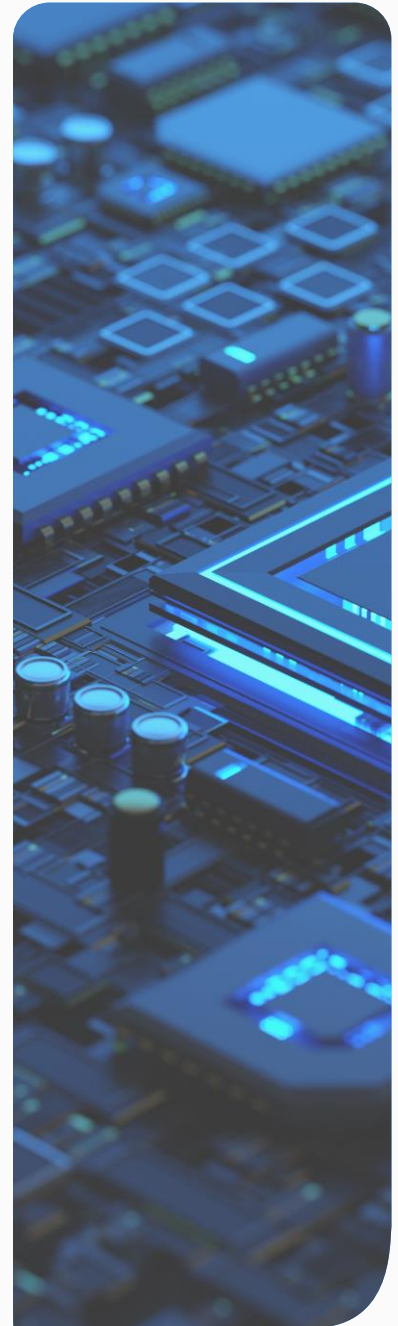
TLP: CLEAR

# Threat Intelligence

**WEEKLY BRIEFING**

Written by: XDR Threat Intelligence Team

Date: 2024-08-16



# 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.

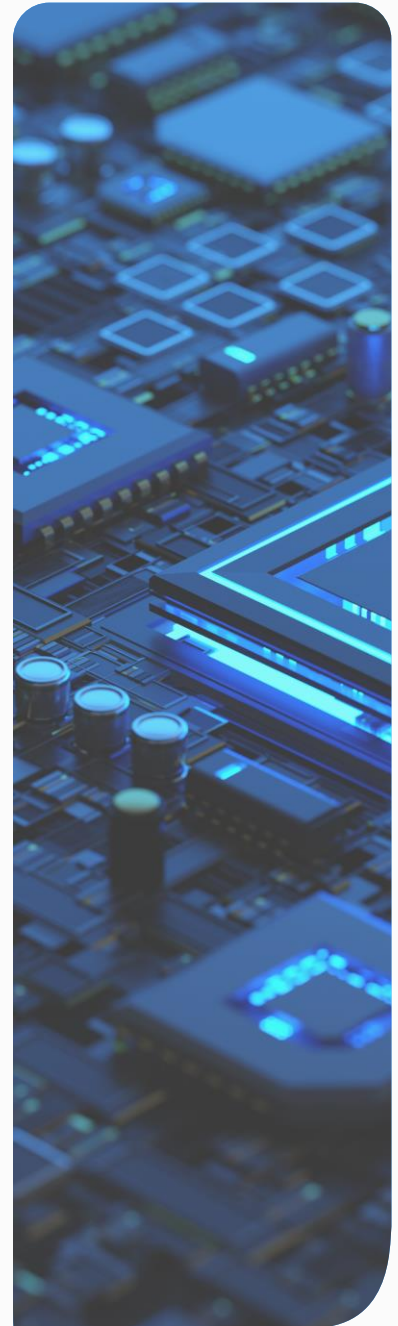
In all cases, Reliance Cyber recommends that, where possible, you closely follow the manufacturer's latest advice to mitigate any vulnerabilities.

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-2024-32113	Apache	OFBiz	07/08/2024
CVE-2024-36971	Android	Kernel	07/08/2024

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.



# Weekly Vulnerability Summary

PRODUCT	CVE ID	CVSS C3 SCORE	Page
Cisco SPA300 & SPA500 Series IP Phones	CVE-2024-20454	9.8	<a href="#">7</a>
SolarWinds Web Help Desk	CVE-2024-28986	9.8	<a href="#">8</a>
WordPress JS Help Desk	CVE-2024-7094	9.8	<a href="#">9</a>
WordPress Appointment Booking Calendar	CVE-2024-7350	9.8	<a href="#">10</a>
Ivanti vTM	CVE-2024-7593	9.8	<a href="#">11</a>



# CVSS Key and Description

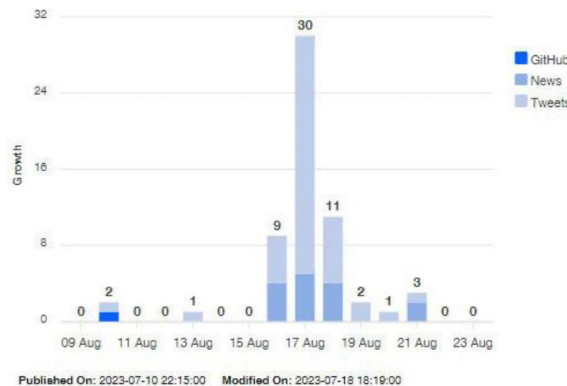
BASE METRIC CATEGORY	DESCRIPTION	OPTION
Attack Vector (AV)	This metric reflects the context by which vulnerability exploitation is possible.	Network Adjacent. Local, Physical
Attack Complexity (AC)	This metric describes the conditions beyond the attacker's control that must exist in order to exploit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

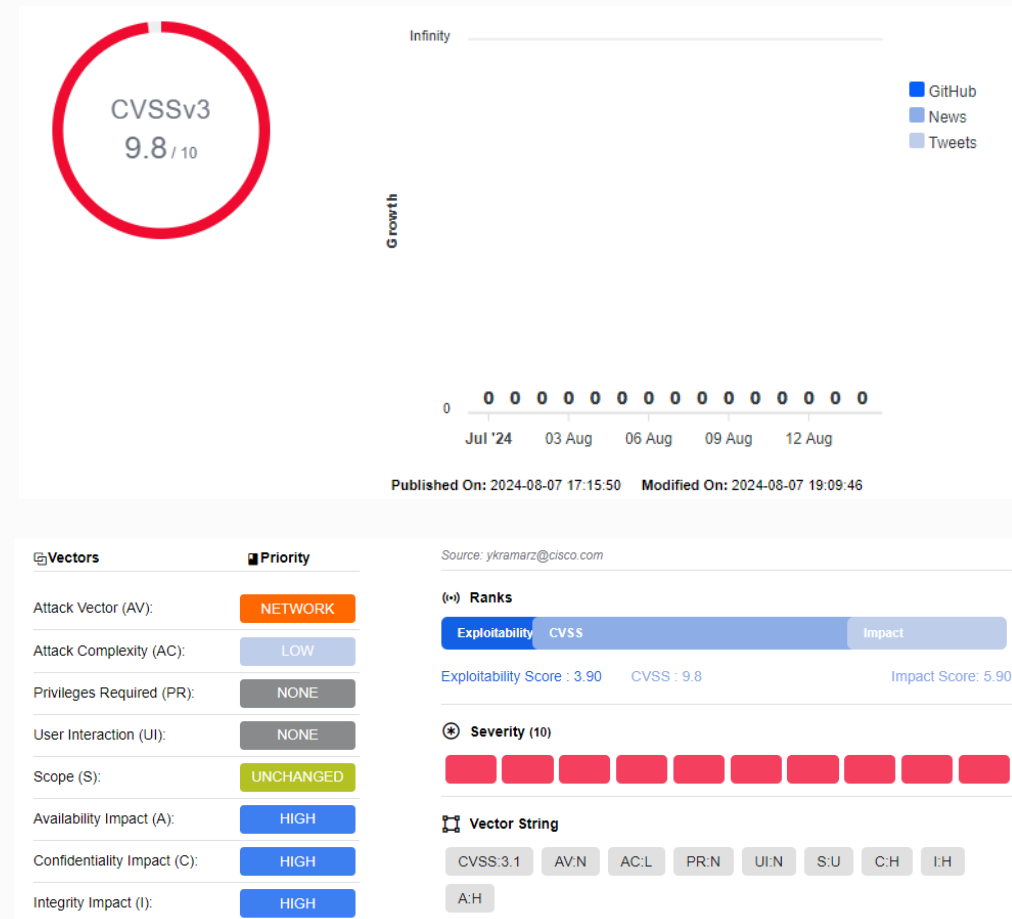
It should be noted that this graphic is NOT showing any deep or dark web traffic regarding any vulnerabilities.

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



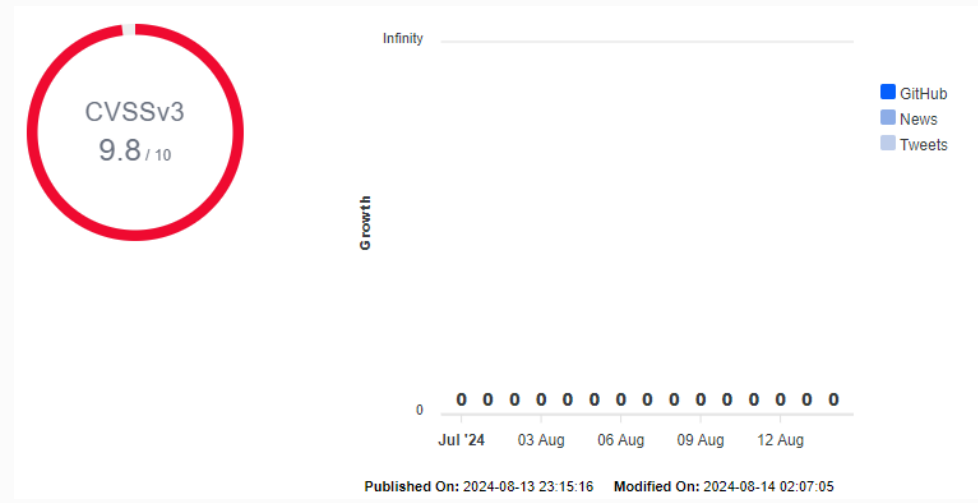
# Cisco SPA300 & SPA500 Series IP Phones Multiple vulnerabilities in MKanagement Interface

<b>CVE ID</b>	<a href="#">CVE-2024-20454</a>
<b>SUMMARY</b>	Multiple vulnerabilities in the web-based management interface of Cisco Small Business SPA300 Series IP Phones and Cisco Small Business SPA500 Series IP Phones could allow an unauthenticated, remote attacker to execute arbitrary commands on the underlying operating system with root privileges. These vulnerabilities exist because incoming HTTP packets are not properly checked for errors, which could result in a buffer overflow. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to overflow an internal buffer and execute arbitrary commands at the root privilege level.
<b>EXPLOITED IN THE WILD</b>	NO
<b>VENDOR SUGGESTED ACTION</b>	Cisco has not released and will not release software updates to address the vulnerabilities that are described in this advisory.
<b>VENDOR RECOMMENDATION</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-http-vulns-RJZmX2Xz">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-http-vulns-RJZmX2Xz</a>



# SolarWinds Web Help Desk Remote Code Execution

CVE ID	<a href="#">CVE-2024-28986</a>
SUMMARY	SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Upgrade to SolarWinds Web Help Desk 12.8.3 HF 1
VENDOR RECOMMENDATION	<a href="https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28986">https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28986</a>



Source: [psirt@solarwinds.com](#)

**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

**Ranks**

Exploitability CVSS Impact

Exploitability Score : 3.90 CVSS : 9.8 Impact Score : 5.90

**Severity (10)**

**Vector String**

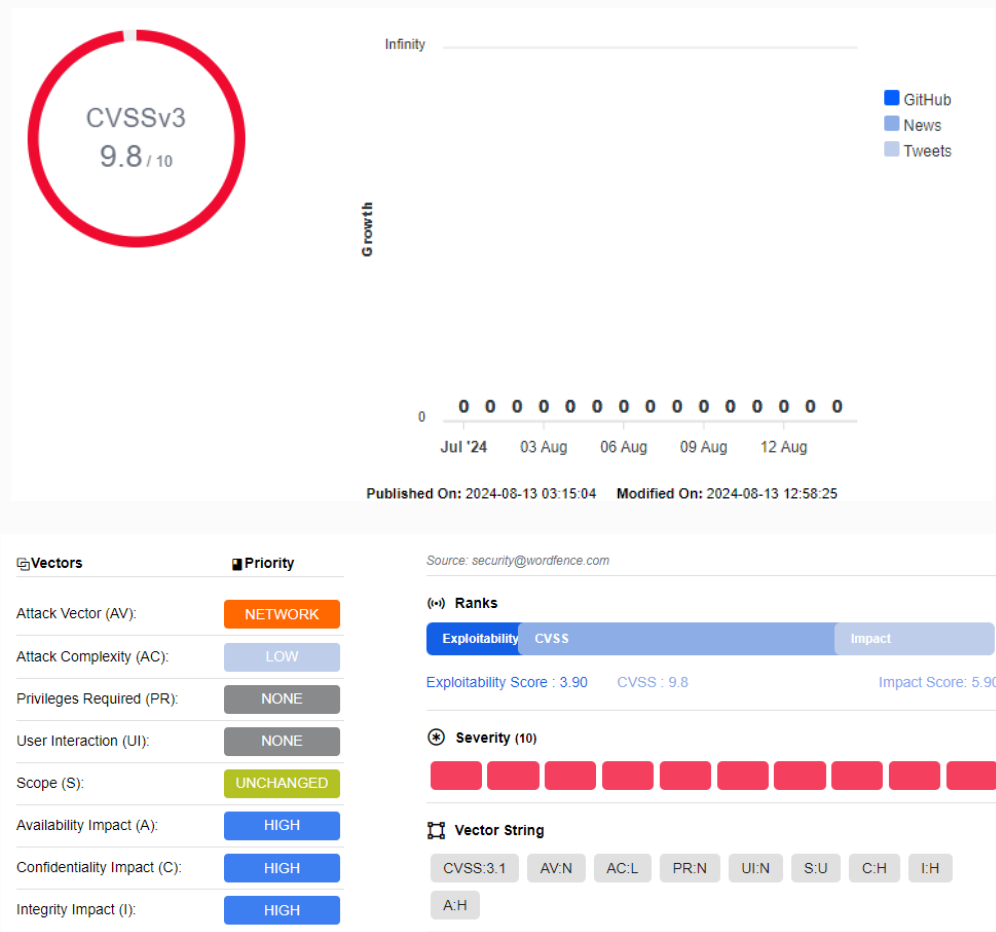
CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H

A:H



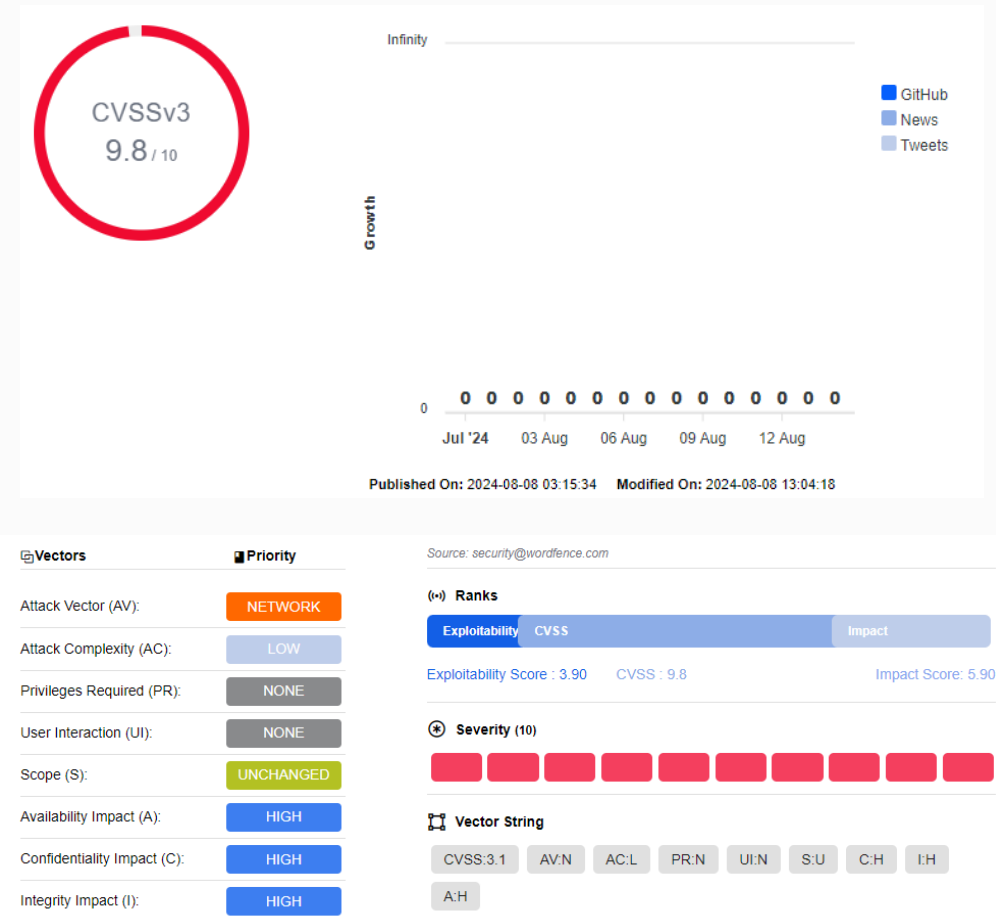
# WordPress JS Help Desk PHP Code Injection

CVE ID	<a href="#">CVE-2024-7094</a>
SUMMARY	The JS Help Desk – The Ultimate Help Desk & Support Plugin for WordPress is vulnerable to PHP Code Injection leading to Remote Code Execution in all versions up to, and including, 2.8.6 via the 'storeTheme' function. This is due to a lack of sanitization on user-supplied values, which replace values in the style.php file, along with missing capability checks. This makes it possible for unauthenticated attackers to execute code on the server. This issue was partially patched in 2.8.6 when the code injection issue was resolved, and fully patched in 2.8.7 when the missing authorization and cross-site request forgery protection was added.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Update to version 2.8.7, or a newer patched version
VENDOR RECOMMENDATION	<a href="https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/js-support-ticket/js-help-desk-the-ultimate-help-desk-support-plugin-286-unauthenticated-php-code-injection-to-remote-code-execution">https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/js-support-ticket/js-help-desk-the-ultimate-help-desk-support-plugin-286-unauthenticated-php-code-injection-to-remote-code-execution</a>




# WordPress Appointment Booking Calendar Authentication Bypass

CVE ID	<a href="#">CVE-2024-7350</a>
SUMMARY	The Appointment Booking Calendar Plugin and Online Scheduling Plugin – BookingPress plugin for WordPress is vulnerable to authentication bypass in versions 1.1.6 to 1.1.7. This is due to the plugin not properly verifying a user's identity prior to logging them in when completing a booking. This makes it possible for unauthenticated attackers to log in as registered users, including administrators, if they have access to that user's email. This is only exploitable when the 'Auto login user after successful booking' setting is enabled.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Update to version 1.1.8, or a newer patched version
VENDOR RECOMMENDATION	<a href="https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/bookingpress-appointment-booking/appointment-booking-calendar-plugin-and-online-scheduling-plugin-bookingpress-116-117-authentication-bypass-to-account-takeover">https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/bookingpress-appointment-booking/appointment-booking-calendar-plugin-and-online-scheduling-plugin-bookingpress-116-117-authentication-bypass-to-account-takeover</a>

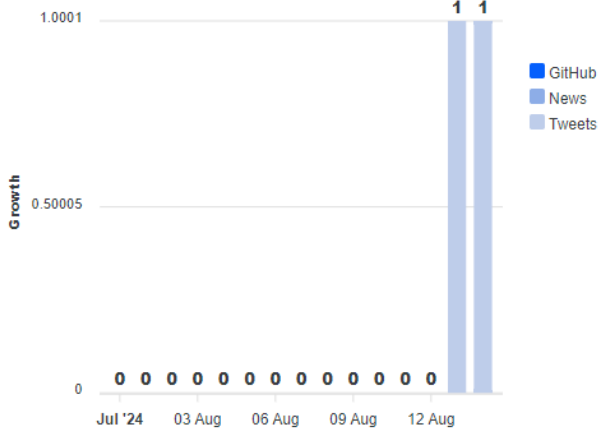


# Ivanti vTM Authentication Bypass

CVE ID	<a href="#">CVE-2024-7593</a>
SUMMARY	Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.
EXPLOITED IN THE WILD	NO
VENDOR SUGGESTED ACTION	Upgrade to the available patch 22.2R1 (released 26 March 2024) or 22.7R2 (released 20 May 2024).
VENDOR RECOMMENDATION	<a href="https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593?language=en_US">https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593?language=en_US</a>



CVSSv3  
9.8 / 10



Growth

1.0001  
0.50005  
0

Jul '24 03 Aug 06 Aug 09 Aug 12 Aug

Legend: GitHub (1), News (1), Tweets (0)

Published On: 2024-08-13 19:15:16 Modified On: 2024-08-14 02:07:05

**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: 3c1d8aa1-5a33-4ea4-8992-aadd6440af75

**Ranks**

Exploitability CVSS Impact

Exploitability Score : 3.90 CVSS : 9.8 Impact Score: 5.90

**Severity (10)**

█ █ █ █ █ █ █ █ █ █

**Vector String**

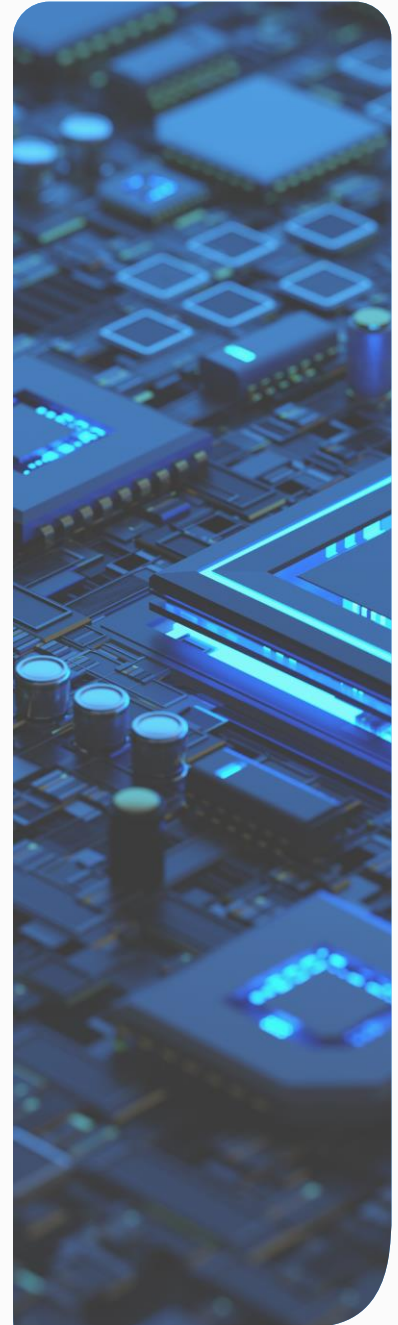
CVSS:3.1 AV:N AC:L PR:N UI:N S:U C:H I:H

A:H

---

TLP: CLEAR

# Threat Intelligence



## Google Patches Critical Android Kernel Zero-Day Exploited in Targeted Attacks

Google recently patched a critical zero-day vulnerability in the Android kernel, identified as [CVE-2024-36971](#). This vulnerability, discovered by Clément Lecigne of Google's Threat Analysis Group, is a use-after-free flaw that allows attackers to execute arbitrary code with elevated privileges.

The flaw was actively exploited in targeted attacks, making it a significant security concern.

### RECOMMENDED ACTION

The August 2024 security update addressed this and 45 other vulnerabilities, highlighting the importance of keeping devices up-to-date with the latest security patches. Therefore please apply the update as soon as is practical.

### SEE ALSO

<https://nordicdefender.com/blog/android-kernel-zero-day-cve-2024-36971>

<https://www.bleepingcomputer.com/news/security/google-fixes-android-kernel-zero-day-exploited-in-targeted-attacks/>

<https://www.techworm.net/2024/08/google-zero-day-kernel-vulnerability.html>

## Royal Ransomware Rebrand as “BlackSuit,” FBI and CISA Release Update to Advisory

The Royal ransomware group has rebranded as "BlackSuit." The FBI and CISA recently released an [updated advisory](#) detailing this change. The advisory highlights the tactics, techniques, and procedures (TTPs) used by BlackSuit, which include phishing emails as a primary method for deploying ransomware and exfiltrating data.

The group has been making ransom demands ranging from \$1 million to \$10 million.

### RECOMMENDED ACTION

**Phishing:** BlackSuit actors most commonly gain initial access to victim networks via phishing emails. See NCSC Advice [here](#).

**RDP:** The second most common vector BlackSuit actors use for initial access is RDP compromise. Microsoft Guidance [here](#).

**Public Apps:** FBI has observed BlackSuit actors gain initial access through exploiting vulnerable public-facing applications. Guidance [here](#).

### SEE ALSO

<https://www.cisa.gov/news-events/alerts/2024/08/07/royal-ransomware-actors-rebrand-blacksuit-fbi-and-cisa-release-update-advisory>

<https://executivegov.com/2024/08/cisa-fbi-cybersecurity-update-warns-of-new-royal-ransomware-tactics/>

<https://www.msn.com/en-us/autos/news/fbi-warns-this-rebranded-ransomware-is-making-some-seriously-high-ransom-demands/ar-AA1osSmt>

## Vulnerabilities in Qualcomm's Adreno GPU Chipsets Affect Billions of Android Devices

Recent reports have highlighted critical security vulnerabilities in Qualcomm's Adreno GPU chipsets, which are used in billions of Android devices. These vulnerabilities, identified by Google researchers, could potentially allow unauthorised access and control over affected devices, posing significant risks to users' data and privacy.

The issues stem from improper memory management within the Adreno GPU driver, leading to memory corruption, information leakage, and arbitrary code execution. Qualcomm has acknowledged these vulnerabilities and is working with device manufacturers to deploy necessary patches.

### RECOMMENDED ACTION

It's crucial for users to keep their devices updated to mitigate these risks.

### SEE ALSO

<https://cybersecuritynews.com/vulnerabilities-in-qualcomms-adreno-gpu-chipset/>

<https://www.techspot.com/news/104215-researchers-uncover-critical-vulnerabilities-qualcomm-adreno-gpu.html>

<https://bing.com/search?q=Vulnerabilities+in+Qualcomm%e2%80%99s+Adreno+GPU+Chipsets+Affect+Billions+of+Android+Devices>

## Hackers Leak 2.7 Billion Data Records with Social Security Numbers

Recently, hackers leaked 2.7 billion records from the U.S., U.K., and Canada containing personal information, including Social Security numbers, on a hacking forum. This data breach is one of the largest in history and includes names, physical addresses, and possible aliases.

The data appears to have been stolen from a background-checking service called [National Public Data](#).

### RECOMMENDED ACTION

If you have any concerns about your personal information, it's a good idea to monitor your credit reports and be vigilant against potential scams and phishing attacks. For additional information please see [NCSC Data breaches: guidance for individuals and families](#)

### SEE ALSO

<https://www.bleepingcomputer.com/news/security/hackers-leak-27-billion-data-records-with-social-security-numbers/>

<https://www.engadget.com/cybersecurity/hackers-may-have-leaked-the-social-security-numbers-of-every-american-150834276.html>

<https://www.theday.com/nation/20240814/hackers-may-have-stolen-the-social-security-numbers-of-every-american-how-to-protect-yourself/>



## Ivanti Releases Updates for Avalanche, Neurons for ITSM, and Virtual Traffic Manager

Ivanti has recently released security updates for several of its products, including Avalanche, Neurons for IT Service Management (ITSM), and Virtual Traffic Manager (vTM). These updates address multiple vulnerabilities that could potentially allow cyber threat actors to take control of affected systems.

The most critical of these vulnerabilities include a SQL injection flaw in Neurons for ITSM and an authentication bypass issue in vT

### RECOMMENDED ACTION

Ivanti strongly recommends users apply these updates promptly to secure their systems.

### SEE ALSO

<https://www.cisa.gov/news-events/alerts/2024/08/13/ivanti-releases-security-updates-avalanche-neurons-itsm-and-virtual-traffic-manager>

<https://forums.ivanti.com/s/article/KB-CVE-2024-22059-and-CVE-2024-22060-for-Ivanti-Neurons-for-ITSM>

<https://www.computing.co.uk/news/4346547/ivanti-patches-critical-flaws-multiple-products>



---

RELIANCECYBER.COM