QUALYSEC
BEYOND CYBERSECURITY

# 2024

## JAN 3RD WEEK

# CYBER SECURITY NEWS


## CONTACT US

www.qualysec.com
865 866 3664
contact@qualysec.com


# New Bluetooth Vulnerability Let Hackers Takeover of iOS, Android, Linux, & MacOS Devices

Bluetooth vulnerabilities in Android, Linux, macOS, iOS, and Windows are critical as hackers could exploit them to gain unauthorized access to the vulnerable devices.

Such flaws in Bluetooth protocols enable the threat actors to steal sensitive data, eavesdrop on communications, and execute malicious actions.

A cybersecurity specialist, Marc Newlin, recently discovered a new Bluetooth vulnerability that enables threat actors to take over iOS, Android, Linux, and MacOS devices.

Also Read: 10 Best Zero Trust Security Vendors – 2024

Bluetooth Vulnerabilities in Android, Linux, macOS, iOS

The threat actors can exploit the new vulnerability without user confirmation to pair an emulated Bluetooth keyboard and inject keystrokes.

Here below, we have mentioned all the vulnerabilities that are discovered by security researchers and affect the iOs, Android, Linux, and macOS:-

- CVE-2024-0230
- CVE-2023-45866
- CVE-2024-21306

**Source : https://cybersecuritynews.com/bluetooth-flaw-hackers-takeover/**

# 1,718,000+ Apache Struts 2 Installation Open to RCE Attacks

Threat actors target Apache Struts 2 due to vulnerabilities in its code that can be exploited for unauthorized access to web applications.

Exploiting these vulnerabilities allows attackers to execute arbitrary code that could lead to full system compromise.

As Apache Struts 2 is widely used in web development, successful attacks can impact many applications, making it an attractive target for those seeking widespread exploits and data breaches.

Cybersecurity researchers at CYFIRMA Research recently discovered more than 1,718,898 Apache Struts 2 installations are open to RCE (Remote code execution) attacks.

The RCE flaw was tracked as "CVE-2023-50164" by security analysts, and this flaw enables threat actors to perform remote code execution and file upload attacks.

Flaw profile

- Vulnerability Type: Unauthenticated Remote Code Execution (RCE) via Apache Struts File Upload
- CVE ID: CVE-2023-50164
- CVSS Severity Score: 9.8 (Critical)
- Application: Apache Struts 2
- Impact: Allows unauthenticated attackers to execute arbitrary code by exploiting a file upload vulnerability
- Severity: Critical
- Affected Versions: Multiple versions of Apache Struts 2 are impacted; refer to the link
- Patch Available: Yes

**Source : https://cybersecuritynews.com/apache-struts-2-rce-attacks/**

# Beware! Hackers Attacking Thousands of Users With Fake iCloud Storage Alert

Since Apple iCloud saves sensitive and personal data like images, emails, and documents, hackers often target Apple iCloud.

Breaching iCloud grants hackers access to sensitive information, allowing them to abuse or sell the data for financial gain and other illicit objectives.

Not only that, but even successful iCloud breaches may also lead to unauthorized access to the connected devices and services.

Cybersecurity analysts at Avast Security recently discovered that hackers actively attack thousands of users with fake iCloud storage alerts.

Fake iCloud Storage Alert

Avast recently warned of a new scam in which hackers are actively attacking thousands of users with fake iCloud storage email alert which states:-

“Your iCloud storage is nearly full”

In this new scam, threat actors primarily targeted users from the following countries:-

- United States of America
- France
- Australia
- Italy
- Spain

**Source : https://cybersecuritynews.com/fake-icloud-storage-alert/**


# Hackers Abuse TeamViewer to Launch Ransomware Attacks

Hackers exploit TeamViewer because it gives remote access to systems and allows threat actors to control them.

This can be used for several illicit purposes like illegal data access, system manipulation, and virus distribution.

Besides this, the widespread use of TeamViewer makes it an attractive target for threat actors who are actively seeking to exploit vulnerabilities and conduct social engineering attacks.

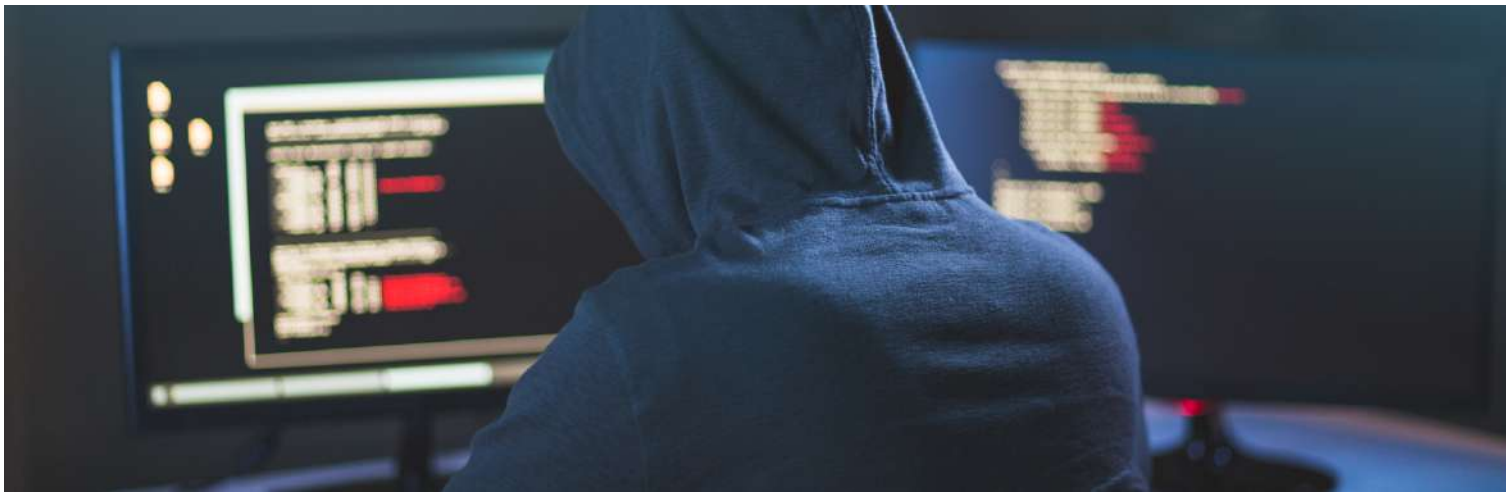
Cybersecurity researchers at Huntress recently identified that threat actors have been actively abusing the TeamViewer to launch ransomware attacks.

Hackers Abuse TeamViewer

The SOC analysts at Huntress recently alerted about 2 endpoints hit by ransomware with minimal impact, no threat actor reconnaissance or lateral movement. However, security software managed to prevent threat actor's actions. The log messages revealed the quarantine of a DLL file that prompted the threat actor to make useless attempts to launch another file that was eventually quarantined.

However, the key security relies on tracking assets by encompassing physical and virtual endpoints and installed apps.

**Source : https://cybersecuritynews.com/hackers-abuse-teamviewer/**



# Pure Malware Tools Masquerade as Legitimate Software to Bypass Detections

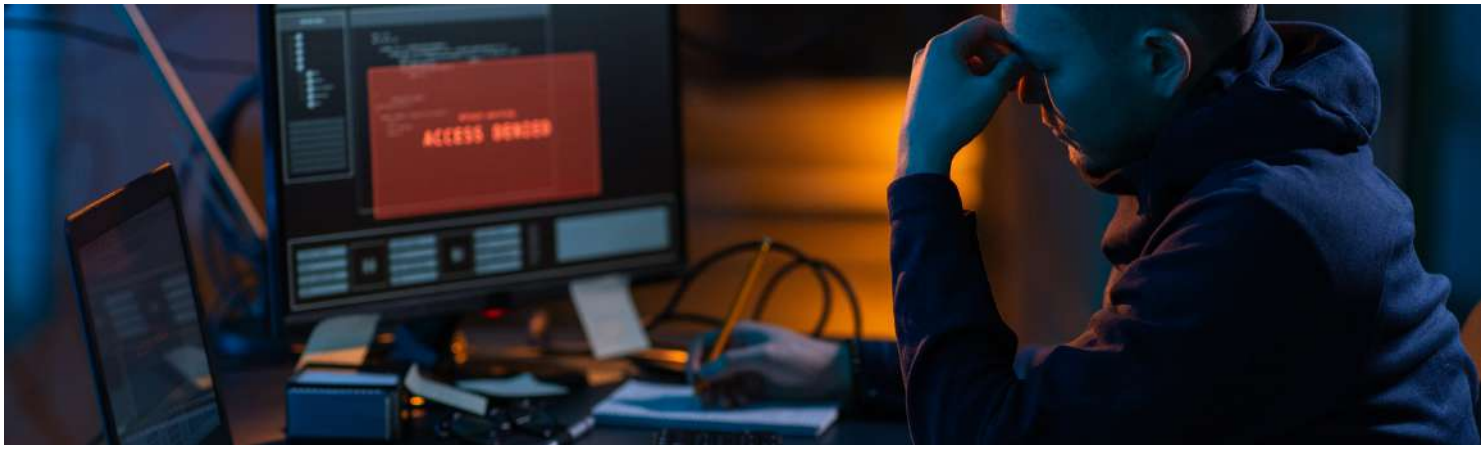
Recently, security analysts at ANY.RUN discovered that the Pure malware tools are masquerading as legitimate software to evade detection.

ANY.RUN is a cloud malware sandbox that handles the heavy lifting of malware analysis for SOC and DFIR teams. Every day, 300,000 professionals use ANY.RUN platform to investigate incidents and streamline threat analysis. If you're a security researcher or an analyst, you can request 14 days of free access to the Any.RUN Enterprise plan.

The PureCoder products were initially distributed in March 2021, as per the developer's old website. While the current Pure site claims that the software is only for education and testing purposes, the observed trend shows that the code is also used for several illicit purposes.The Pure updates since March 2023 mentioned the Telegram bot sales. While the bots automate and anonymize malware purchases, The author expands the service, explores new channels, and scales up through bot usage.

Recently, in Q4, ANY.RUN discovered the use of T1036.005 in over 98,500 malicious samples. You can see what the top malware families, Types, Tactics, Techniques, and Procedures (TTPs) used by attackers in 2023 can tell us about what to expect in 2024.

**Source : https://cybersecuritynews.com/pure-malware-tools/**



# New iShutdown Scripts Enable Detection of Spyware On iPhones

Malware hunting on iOS devices has been extremely difficult due to the nature of the iOS ecosystem.

There were only two methods for conducting forensic investigations on iOS devices: either to examine an encrypted full iOS backup or analyze the network traffic of the suspected device.

However, both methods require a lot of time and money and are quite complicated. As a result, several threats might go undetected.

Moreover, Some of the iPhone devices were investigated as part of general security checks that were found with traces of Pegasus malware infections. Overview of the detection – Shutdown.log

According to the reports shared with Cyber Security News, Shutdown.log is a text-based log file that logs every reboot event on iOS devices. This file consists of multiple environment characteristics that date back several years and provide a lot of information.

During the analysis of the infected phones, the MVT tool detected the malware by parsing the DataUsage database, among other forensic artifacts that can be investigated.

As a means of investigation, network traffic analysis was initially suggested, which is an effective method but requires a lot of expertise and resources.

**Source :https://cybersecuritynews.com/new-ishutdown-scripts/**

# LeftoverLocals Attack Let Attackers Steal AI Data From Apple, Qualcomm & AMD GPUs

An attacker may be able to steal a significant amount of data from a GPU's memory due to a flaw known as LeftoverLocals that affects several popular GPU brands and models, including AMD, Apple, and Qualcomm.

Machine learning (ML) models and large language models (LLMs) operating on affected GPU platforms are especially affected by LeftoverLocals, which negatively impacts GPU apps' security posture.

It is also found that while Arm, Intel, and Nvidia products are unaffected, the GPUs manufactured by Imagination Technologies are also impacted.

Details of the 'LeftoverLocals' Attack

Researchers Tyler Sorensen and Heidy Khlaaf of Trail of Bits found the vulnerability, which they named LeftoverLocals and tracked as CVE-2023-4969.

LeftoverLocals allows data recovery from GPU local memory created by another process on Apple, Qualcomm, AMD, and Imagination GPUs.

Hackers can leverage the issue to gain access to data that they should not have access to, such as requests and responses created by LLMs, as well as the weights that drive the response.

Researchers demonstrated how they could conduct an attack on an interactive LLM chat session using LeftoverLocals. A co-resident attacker can hear the LLM's response when the LLM user asks a query of the LLM.

**Source :https://cybersecuritynews.com/leftoverlocals-attack/**

# Iranian Mint Sandstorm Attacking Researchers With New Hacking Tools

Hackers frequently target researchers to get illegal access to important research data, intellectual property, and highly sensitive information.

The threat actors can exploit this information for various illicit purposes like economic espionage, competitive advantage, or selling the data on the black market.

Cybersecurity researchers at Microsoft recently discovered that the threat actors behind Mint Sandstorm are actively attacking the researchers with new hacking tools.

Mint Sandstorm (PHOSPHORUS), which is linked to Iran's IRGC, has been actively targeting high-profile individuals at universities and research organizations in Belgium, France, Gaza, Israel, the UK, and the US since November 2023 using custom phishing to deploy MediaPl backdoor.

The operators of this threat group are highly skilled social engineers as they adapt and persist in compromised environments, which poses a serious threat to security.

**Source : https://cybersecuritynews.com/mint-sandstorm-attacking-researchers/**


# MyFlaw – Opera Bug Let Hackers Run ANY File on Mac or Windows

Hackers exploit Remote Code Execution (RCE) vulnerabilities as they allow them to execute arbitrary code on a target system remotely.

This unauthorized access enables the threat actors to take control of the system and perform a multitude of illicit activities.

Recently, cybersecurity researchers at Guardio Labs discovered an Opera bug that lets hackers run any file on Mac and Windows. This newly discovered flaw has been dubbed as “MyFlaw.”

Opera’s My-Flow

Opera’s My Flow is a file-sharing system that flawlessly syncs notes and files across desktop and mobile via its browser. This file-sharing system enables its users to scan a QR code on the mobile app for instant chat-style sharing.

The chat interface in Opera’s My Flow allows immediate file execution via an ‘OPEN’ link, raising high-risk security issues. Researchers investigated the potential vulnerabilities that revealed a significant flaw in the system’s architecture and security protocols.

Opera is constructed on the Chromium open-source project that shares the core code and design. Opera leverages Chromium’s customization, including built-in browser extensions with enhanced features to stand out.

**Source : https://cybersecuritynews.com/myflaw-opera-bug/**

# 178,000+ Publicly Exposed Sonicwall Firewalls Vulnerable to RCE Attacks

Due to Sonicwall Firewalls' widespread usage in organizations, hackers find them to be appealing targets when looking to breach networks.

By taking advantage of security holes in Sonicwall Firewalls, malicious users can get unwanted access to confidential data, make it easier for outsiders to infiltrate networks, and launch several kinds of cyberattacks.

Cybersecurity researchers at Bishopfox recently discovered 178,000 vulnerable Sonicwall firewalls that could be exploited by the threat actors in the wild.

Sonicwall Firewall Vulnerable to RCE Attacks

SonicWall NGFW series 6 and 7 faces unauthenticated DoS vulnerabilities (CVE-2022-22274, CVE-2023-0656), potentially allowing remote code execution.

However, no wild exploitation was reported, but a POC for CVE-2023-0656 is public. The BinaryEdge data shows 76% of exposed SonicWall firewalls (178,637 of 233,984) vulnerable. The impact of a widespread attack could be severe as the default SonicOS restarts after a crash, but three crashes lead to maintenance mode.

**Source : https://cybersecuritynews.com/sonicwall-firewalls-rce-attack/**

# Google Chrome Browser Zero-Day Vulnerability Exploited in Wild

Google Chrome released the first security update in 2024 with a fix for the zero-day bug actively exploited in Wild.

An update to Google Chrome 120.0.6099.234 for Mac, 120.0.6099.224 for Linux, and 120.0.6099.224/225 for Windows will be released in the next days or weeks.

Hackers exploit zero-day flaws as these vulnerabilities are unknown to software vendors, making them valuable for launching attacks before security patches are developed.

Even exploiting zero-day flaws can provide a strategic advantage to the threat actors in launching targeted and undetected attacks.

Recently, the following cybersecurity researchers identified multiple vulnerabilities, along with a zero-day flaw exploited in the wild:

- CVE-2024-0517 Reported by Toan (suto) Pham of Qrious Secure on 2024-01-06
- CVE-2024-0518 Reported by Ganjiang Zhou (@refrain_areu) of ChaMd5-H1 team on 2023-12-03
- CVE-2024-0519 Reported by Anonymous on 2024-01-11

The zero-day exploit (CVE-2024-0519) hits the V8 JavaScript engine with out-of-bounds memory access.

**Source : https://cybersecuritynews.com/google-chrome-browser-zero-day-vulnerability/**

# Hackers Exploiting Windows Defender SmartScreen Flaw to Hijack Computers

Hackers actively target and exploit Windows Defender SmartScreen to deceive users and deliver malicious content by creating convincing, misleading websites or applications.

By evading SmartScreen, the threat actors increase the chances of their malicious content being executed on users' systems to compromise security.

This exploitation often involves the use of social engineering tactics to deceive users and bypass the protective features of SmartScreen.

Recently, cybersecurity researchers at Trend Micro discovered that hackers are actively exploiting the Windows Defender SmartScreen flaw, which is tracked as "CVE-2023-36025," to hijack Windows machines.

Flaw profile

- CVE ID: CVE-2023-36025
- Description: Windows SmartScreen Security Feature Bypass Vulnerability
- Released: Nov 14, 2023
- Last updated: Nov 22, 2023
- CVSS:3.1 8.8 / 8.2

**Source :https://cybersecuritynews.com/windows-defender-smartscreen-flaw/**

**“It is crucial for users to exercise caution when receiving spam emails or to visit phishing websites and to verify the source before downloading any applications”, concludes the researchers.**

It's a fact that cybercrime is on the rise and it's more important than ever to protect your business from cyber threats.

But the good news is that you don't have to navigate the complex world of cybersecurity alone. Our team of experts is here to help you cyber security testing services need to protect your application or business.

Don't wait for a cyber attack to happen. Contact us now to learn more about how we can help secure your business and give you peace of mind.

**Contact now and protect your business with our expert cyber security services.**

## CONTACT US AT