QUALYSEC
BEYOND CYBERSECURITY

2024

MAR 2ND WEEK

CYBER SECURITY NEWS

CONTACT US

www.qualysec.com

865 866 3664

contact@qualysec.com

Vulnerability in 150K+ Fortinet Devices Let Hackers Execute Arbitary Code Remotely

A recent investigation has uncovered a flaw in internet-connected doorbell cameras, specifically affecting Ivanti's Pulse Secure appliances.

The NVISO Incident Response team discovered the discovery, which identified two covert TLS-based backdoors, SparkCockpit and SparkTar, allowing attackers to hijack these devices and gain unauthorized access to internal networks.

The investigation was triggered by a critical-sector organization that observed a compromise of their Ivanti appliance, leading to the discovery of these sophisticated backdoors.

Sophisticated Attack Techniques

Both SparkCockpit and SparkTar employ selective interception of TLS communication towards legitimate Ivanti server applications, which helps them avoid detection.

SparkTar is particularly advanced and capable of surviving factory resets and appliance upgrades.

It also allows for file uploads, command execution, and setting up SOCKS proxies to relay attacker traffic directly into the organization's network.

Source : https://cybersecuritynews.com/fortinet-devices-vulnerable/

Russian Spies Hacked Microsoft Email Systems & Stolen Source Codes

Microsoft has disclosed that Russian government hackers, identified as the group Midnight Blizzard, have successfully infiltrated its corporate email systems and stolen source codes.

The tech giant recently discovered unauthorized access attempts that were made using information obtained from a previous hack that took place last year. This ongoing cyberattack highlights the continuous threat caused by nation-state actors and raises serious concerns regarding the security of crucial technological infrastructure.

Microsoft's announcement on March 8, 2024, detailed that Midnight Blizzard, also known as APT29 or Cozy Bear, utilized information initially exfiltrated from the company's corporate email systems to gain unauthorized access to its internal systems, including source code repositories.

This breach is part of a series of intrusions that began in November of the previous year, targeting the corporate email accounts of senior leadership and employees across various departments, including cybersecurity and legal functions. The hackers seem to have multiple objectives, including stealing valuable source codes and gathering intelligence on Microsoft's knowledge about their operations.

Source : https://cybersecuritynews.com/russian-spies-hacked-microsoft/

Gitlab Authorization Bypass Vulnerability Let Attackers Steal Protected Variables

GitLab has announced the release of updated versions for its Community Edition (CE) and Enterprise Edition (EE) platforms. These updates address critical vulnerabilities that could allow attackers to bypass authorization mechanisms and access protected variables.

The updates, versions 16.9.2, 16.8.4, and 16.7.7, come as a response to the discovery of two major security flaws, CVE-2024-0199 and CVE-2024-1299, which posed a high risk to the integrity and confidentiality of data managed through the GitLab platform.

GitLab has strongly urged all users to upgrade their installations to these latest versions to mitigate the risks associated with these vulnerabilities.

The company has already updated GitLab.com to the patched version, ensuring that online platform users are protected from these security flaws.

Understanding the Vulnerabilities

CVE-2024-0199: A High Severity Threat

The more critical of the two, CVE-2024-0199, was identified as an authorization bypass vulnerability affecting a wide range of GitLab versions – from 11.3 up to the versions immediately preceding the patched releases.

Source : https://cybersecuritynews.com/gitlab-vulnerability-attackers-steal/

Android Malware-as-a-Service “Coper” Offering Advanced Features to Hackers

The Coper malware, a descendant of the Exobot malware family, was first distributed as a fake version of Bancolombia’s ‘Personas’ application.

Fast forwarding to 2022, the malware was discovered, and a lite version of the same malware was advertised on underground forums under the name “Octo Android botnet”.

However, the malware has been presently found to be offered as a malware-as-a-service in which customers are provided with access to a panel and builder used for executing the campaigns.

Moreover, the malware is capable of keylogging, interception of push notifications and SMS messages, as well as control over the infected device’s screen.

Android Malware-as-a-Service

According to the reports shared with Cyber Security News, the evolution of the malware started in 2021 when it targeted Colombian Android users using several tactics, including impersonation of legitimate banking applications and other applications to create trust with victims for installation.

Source : https://cybersecuritynews.com/android-malware-as-a-service/

Snort 2.9.8.3 and Snort 2.9.13.0 End of Life for Talos Rules

The end-of-life for Talos rules support for two versions of the widespread intrusion detection and prevention system Snort has been declared.

Effective immediately, the rule set for Snort version 2.9.8.3 is no longer available.

Users of this version must note that they will not receive any further updates or security patches, which could leave their systems vulnerable to new threats.

For those utilizing Snort 2.9.13.0, the clock is ticking. Talos rules for this version will cease on or around July 1, 2024.

This timeline allows users to transition to newer versions of Snort, ensuring continued protection against cyber threats.

Upgrading to Snort 3

In light of these changes, the open-source community is strongly encouraged to upgrade to Snort 3, the latest version. This version offers enhanced capabilities, improved performance, and the latest security features.

Users can download Snort 3 from the official Snort downloads page.

For users who prefer to stick with Snort 2, it is recommended that they update to Snort 2.9.20 as soon as possible.

Source : https://cybersecuritynews.com/snort-end-of-life-for-talos-rules/

FBI Releases Internet Crime Report for 2023 : 22% Surge Compared to 2022

Federal Bureau of Investigation (FBI) has published its annual Internet Crime Report for 2023, highlighting a significant 22% increase in losses due to cybercrime, amounting to over $12.5 billion

This surge underscores cyber criminals' growing sophistication and audacity in exploiting digital vulnerabilities.

The Internet Crime Complaint Center (IC3), a pivotal arm of the FBI dedicated to combating cybercrime, registered an unprecedented 880,418 complaints from the American public in 2023.

This figure marks a nearly 10% increase in the number of complaints received and represents a staggering 22% rise in financial losses compared to the previous year.

Timothy Langan, Executive Assistant Director at the FBI, emphasized the conservative nature of these figures, suggesting the actual scope of cybercrime is likely much broader.

The IC3's Role in Combating Cyber Crime

The IC3 serves as a central hub for victims to report cybercrime and for the FBI to collect data, advance investigations, and identify changes in the threat landscape.

Source : https://cybersecuritynews.com/fbi-releases-crime/

Zama Raises $73M in Series A Lead by Multicoin Capital and Protocol Labs to Commercialize Fully Homomorphic Encryption

Company Open Sources FHE Libraries to Build Privacy-Preserving Blockchain and AI Applications for the First Time.

An investment has been secured to bring Fully Homomorphic Encryption (FHE) to the fore, allowing developers to address data privacy challenges across blockchain and AI use cases.

Zama, an open-source cryptography company building state-of-the-art FHE solutions to protect privacy in blockchain and AI, today announced a $73M Series A round led by Multicoin Capital and Protocol Labs, with participation from Metaplanet, Blockchange Ventures, VSquared, and Stake Capital, as well as blockchain pioneers Juan Benet (founder of Filecoin), Anatoly Yakovenko (co-founder of Solana), and Gavin Wood (co-founder of Ethereum and co-creator of Polkadot).

The funds will be used to hire talented engineers, software developers, and researchers in cryptography, maintain its open-source libraries, and collaborate with strategic partners to develop a new class of Fully Homomorphic Encryption (FHE) applications.

As demand for robust data protection grows internationally, businesses and organizations need a way to protect consumer data without compromising its utility.

Source : https://cybersecuritynews.com/zama-raises-73m-in-series/

TA4903 Hackers Spoofing U.S. Government Entities To Steal Corporate Credentials

TA4903 is a financially motivated cybercriminal threat actor who impersonates both US government institutions and private businesses across a wide range of industries.

The actor mostly targets organizations in the United States but occasionally those worldwide through high-volume email campaigns.

The campaign's goals are to obtain corporate credentials, hack mailboxes, and carry out subsequent business email compromise (BEC) activities.

Proofpoint Researchers noticed an upsurge in credential phishing and fraud attempts employing various TA4903 themes from mid-2023 to 2024. The actor began spoofing small and medium-sized enterprises (SMBs) across a range of sectors, including manufacturing, energy, finance, food and beverage, and construction.

The rapid growth of BEC themes also increased, with themes like "cyberattacks" being used to entice victims to disclose their banking and payment information. "The actor's recent BEC campaigns that move away from government spoofing and instead purport to be from small and medium-sized businesses have become more frequent", Proofpoint shared with Cyber Security News.

Source : https://cybersecuritynews.com/hackers-spoofing-u-s-government/

New xStealer Malware Debuted With Advanced Features

A new player has emerged with capabilities that pose risks to digital security. Dubbed xStealer, this malware has been designed to stay ahead of the curve with continuous updates and enhancements, ensuring it remains at the forefront of data-stealing technology.

xStealer is not just another addition to the plethora of cyber threats; it represents a sophisticated evolution in malware design.

According to recent reports, the xStealer malware has been equipped with an array of advanced features that enable it to siphon sensitive information with alarming efficiency.

Persistent and Evolving

One of the most concerning aspects of xStealer is its commitment to growth. The developers behind this malware have promised constant updates, ensuring that it stays updated with the latest and greatest in stealer technology. This includes compatibility with new applications, software patches, and other enhancements that could bypass traditional security measures. ThreatMon has recently tweeted about the latest updates to xStealer malware. According to the announcement, xStealer now includes additional features that enable it to efficiently steal sensitive data.

Source : https://cybersecuritynews.com/xstealer-malware-debuted/

Cisco Secure Client Flaw let Attackers Trigger CRLF Injection Attack

Cisco has disclosed a critical vulnerability in the SAML authentication process of its Cisco Secure Client software. This vulnerability could potentially allow unauthenticated, remote attackers to conduct a Carriage Return Line Feed (CRLF) injection attack.

This flaw poses a significant risk to users by enabling attackers to execute arbitrary script code in the user's browser or access sensitive information.

Understanding the Vulnerability

The vulnerability, identified due to insufficient validation of user-supplied input, can be exploited by an attacker by persuading a user to click on a specially crafted link while establishing a VPN session.

If successful, the attacker could leverage this to execute arbitrary script code in the browser or access sensitive, browser-based information, including valid SAML tokens.

These tokens could then be used to establish a remote access VPN session with the privileges of the affected user. However, individual hosts and services behind the VPN headend would still require additional credentials for access.

Source : https://cybersecuritynews.com/cisco-secure-flaw-attack/

Beware Of New Money Laundering Attack Targeting UPI Users

Threat actors target UPI users as UPI offers a convenient platform for transferring money, often with less severe security than traditional banking systems.

Due to fewer security measures, threat actors exploit user behavior and transaction process vulnerabilities to commit fraud, steal sensitive information, and carry out financial scams.

Cybersecurity researchers at CloudSEK recently discovered that the widespread use and relatively lower security measures of UPI attract threat actors to perform money laundering attacks to target UPI users. Successful exploitation allows threat actors to illicitly transfer funds, leveraging UPI transactions' anonymity and ease of use.

UPI Money Laundering Alert. A money mule is crucial in facilitating financial crimes, like cyber fraud or money laundering, by receiving and transferring funds obtained through fraud. CloudSEK uncovered a significant loophole in India's banking system in October 2023. Chinese threat actors actively exploited this flaw to run a massive money laundering scheme by utilizing a vast network of compromised "money mule" accounts to channel illicit funds through fraudulent payment channels.

Source : https://cybersecuritynews.com/upi-money-laundering-alert/

30,000+ Individuals Impacted in Fidelity Investments Third-party Data Breach

Over 30,000 individuals have been left vulnerable after a third-party data breach involving Fidelity Investments Life Insurance Company (FILI).

The breach, orchestrated through Infosys McCamish (IMS), a third-party service provider, has raised serious concerns about the security measures to protect sensitive customer information.

A Breach of Trust and Data

Fidelity Investments, a cornerstone in the financial services sector, found itself precarious when IMS notified them in November of a "cybersecurity event" that had severely disrupted its services.

An investigation conducted with a third-party firm's assistance revealed that IMS's systems were compromised between October 29 and November 2. The breach allowed unauthorized access to critical data, including names, Social Security numbers, states of residence, and even bank account details. Jeff Margolies, chief product and strategy officer at Saviynt, emphasized the growing threat of third-party breaches, stating, "Enterprises are highly reliant on third-party service providers, who are now often the easiest vector into an enterprise's most critical data."

Source : https://cybersecuritynews.com/30000-investments-data-breach/

ArubaOS Security Flaw Let Attackers Execute Remote Code

ArubaOS-Switch belongs to Aruba Networks and it's a subsidiary of HPE (Hewlett Packard Enterprise).

It helps centralize network management, and besides this, it also develops diverse products related to networking.

Security Analysts Discovered a multitude of vulnerabilities in ArubaOS-Switch Switches, including CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613, CVE-2024-25614, CVE-2024-25615, and CVE-2024-25616.

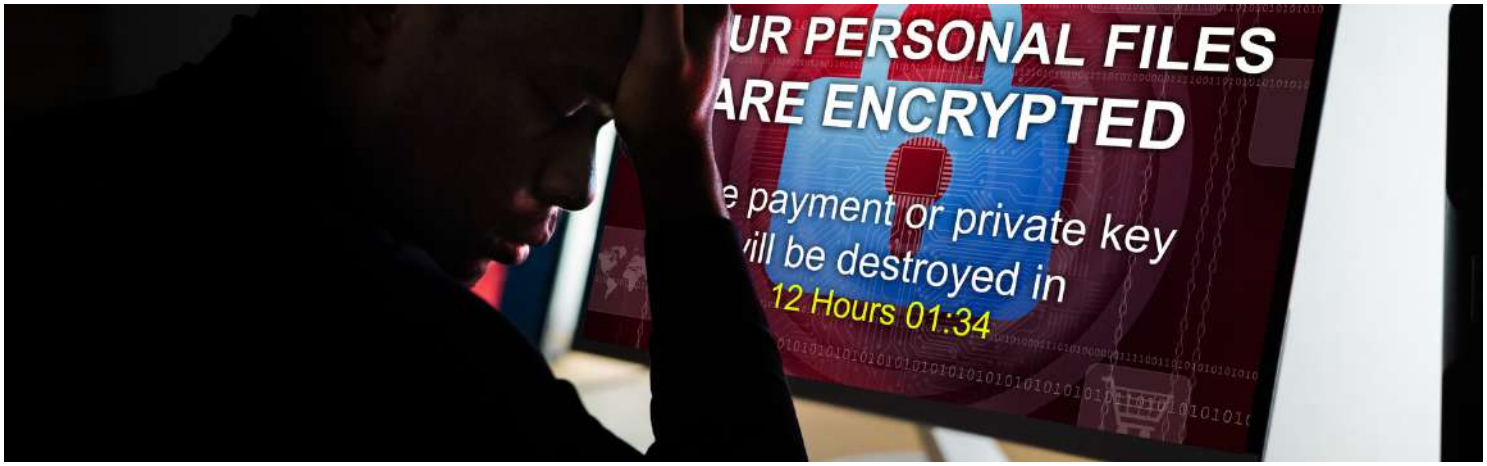
However, to mitigate these vulnerabilities, HPE Aruba Networking has released patches for ArubaOS.

Flaws' Profiles

Here below we have mentioned all the vulnerabilities:-

- Authenticated Remote Command Execution in the ArubaOS Command Line Interface (CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613)
- Description: ArubaOS CLI has command injection flaws. Exploits let attackers run arbitrary commands as privileged OS user.
- Severity: High

Source :https://cybersecuritynews.com/arubaos-remote-code-execution-flaw/



Microsoft .NET Framework & Visual Studio Flaw Let Attackers Write or Delete Files

A vulnerability, CVE-2023-36049 has been identified in the Microsoft .NET Framework and Visual Studio, posing a serious threat to the integrity of FTP servers.

If exploited, this flaw could allow attackers to write or delete files, compromising the security of applications and data.

The .NET Framework, a cornerstone of software development on Microsoft Windows, facilitates the creation and execution of applications within a managed execution environment.

However, a flaw in its design related to handling FTP commands has opened a door for cyber attackers.

FTP, or File Transfer Protocol, is a standard network protocol for transferring computer files between a client and server on a computer network.

It operates on a dual-connection system, one for commands and the other for data transfer.

The vulnerability stems from the .NET Framework's improper user input validation, specifically in how FTP command parameters and FTP URI requests are processed.

Source :https://cybersecuritynews.com/microsoft-net-framework-visual-studio-flaw/

Cisco Duo for Windows Logon and RDP Let Attacker Bypass Authentication

A critical vulnerability, CVE-2024-20301 has been identified in Cisco Duo Authentication for Windows Logon and Remote Desktop Protocol (RDP), posing a security risk to affected systems.

This flaw could allow an authenticated, local attacker to bypass secondary authentication mechanisms and gain unauthorized access to Windows devices.

The vulnerability stems from a failure to invalidate locally created trusted sessions after a device reboot, enabling attackers with primary user credentials to exploit this weakness successfully.

The vulnerability impacts Cisco Duo Authentication for Windows Logon and RDP versions 4.2.0 through 4.2.2. Systems running earlier versions than 4.2.0 or the latest patched version, 4.3.0, are not vulnerable to this exploit.

The risk associated with this vulnerability is exceptionally high due to the potential for attackers to gain access to sensitive information and systems without valid permissions, posing a significant threat to organizational security and data integrity.

Cisco's Response and Software Updates- In response to the discovery of this vulnerability, Cisco has released software updates to address the issue, with no workarounds available.

Source : https://cybersecuritynews.com/cisco-duo-windows-attacker/

Copybara Uses On-Device Fraud to Steal Funds Directly from the Victim's Device

Cybersecurity experts at Cleafy Labs have exposed a sophisticated fraud campaign orchestrated by a group known as Copybara.

This campaign, leveraging on-device fraud techniques, has been meticulously designed to siphon funds directly from victims' devices, marking a significant escalation in the severity and sophistication of cyber threats facing individuals and institutions alike.

Cleafy Labs detailed the Copybara campaign, which employs a multifaceted approach to infiltrate and exploit victims' devices.

Unlike traditional fraud methods that rely on intercepting or redirecting communications between a user and their financial institution, on-device fraud occurs directly within the compromised device.

This method allows attackers to bypass many of the security measures that banks and other financial services have put in place, making it a particularly insidious form of cybercrime.

Copybara Uses On-Device Fraud to Steal Funds

At the heart of the Capybara campaign is malicious software, or malware, that is cleverly disguised within seemingly innocuous applications.

Source : https://cybersecuritynews.com/copybara-uses-on-device/

“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