Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 69b94867 | Oct 27, 2023, 07:21 AM

Today's Headlines:

Leading Story

- Critical Mirth Connect Vulnerability Could Expose Sensitive Healthcare Data

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- France Says Russian State Hackers Breached Numerous Critical Networks
- StripedFly Malware Framework Infects 1 Million Windows, and Linux Hosts

Vulnerabilities & Exploits

- F5 Issues Warning: BIG-IP Vulnerability Allows Remote Code Execution

Trends & Reports

- Cloudflare Sees Surge in Hyper-Volumetric HTTP DDoS Attacks
- IoT Security Threats Highlight the Need for Zero Trust Principles

Privacy, Legal & Regulatory

- CISA Releases Cybersecurity Toolkit for Healthcare

Cybersecurity Awareness Month

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

Critical Mirth Connect Vulnerability Could Expose Sensitive Healthcare Data

Summary

- Users of Mirth Connect are at risk of private data being exposed because of a remote code execution vulnerability being found within the software.

Analysis & Action

Horizon3.ai warns users of Mirth Connect of CVE-2023-43208, a remote code execution vulnerability affecting Mirth Connect's software, that could be used to expose private healthcare data. The vulnerability is affecting all Mirth Connect versions.

The new vulnerability, CVE-2023-43208 is a bypass for the vulnerability tracked as CVE-2023-37679 reported and patched some months ago. Currently, there are more than 1,200 Mirth Connect instances exposed on the internet, putting healthcare facilities that use Mirth Connect at risk of threat actors accessing and extracting personal healthcare data. NextGen HealthCare released Mirth Connect version 4.4.1 to patch up the vulnerability.

Members who use Mirth Connect are highly encouraged to update their systems to version 4.4.1 as soon as possible to prevent private data and information from being extracted.

Data Breaches & Data Leaks

Nothing to Report.

Cyber Crimes & Incidents

France Says Russian State Hackers Breached Numerous Critical Networks

Summary

- Russian APT28 hacking group has been linked to the exploitation of two new vulnerabilities.

Analysis & Action

Considered to be part of Russia's military intelligence service, APT28, also known as Fancy Bear, has been targeting peripheral devices on critical networks of French organizations since 2021, and has been linked to the exploitation of two vulnerabilities.

The first, CVE-2023-38821, is a remote code execution vulnerability in WinRAR. The second, CVS-2023-23397, is a zero-day privilege elevation flaw in Microsoft Outlook.

The French National Agency for the Security of Information Systems (ANSSI) conducted investigations on Fancy Bear's techniques, tactics, and procedures (TTPs) and found they used brute force along with leaked databases with credentials to compromise accounts. It has been revealed that the group also used a wide variety of VPN clients.

Members should use secure communication platforms to prevent email diversions or hijacks and minimize the attack surface of webmail interfaces to ensure the security and confidentiality of email exchanges.

StripedFly Malware Framework Infects 1 Million Windows, Linux Hosts

Summary

- A sophisticated malware platform that flew under the radar of cybersecurity researchers for five years infected over a million Windows and Linux systems during that time.

Analysis & Action

The malware platform is named StripedFly and was wrongly classified as just a Monero cryptocurrency miner.

Analysts have discovered that the malware features sophisticated TOR-based traffic concealing mechanisms, automated updating from trusted platforms, worm-like spreading capabilities, and a custom EternalBlue Server Message Block version 1 (SMBV1) exploit. It is unclear if the malware network is utilized for revenue generation or cyber espionage, but its sophistication indicates that it is an advanced persistent threat (APT) malware.

Members are advised to utilize caution when downloading software onto devices connected to their network. If possible, members are also advised to disable SMB on critical devices.

Vulnerabilities & Exploits

F5 Issues Warning: BIG-IP Vulnerability Allows Remote Code Execution

Summary

- F5 is warning customers about a critical security vulnerability affecting BIG-IP, tracked as CVE-2023-46747.

Analysis & Action

F5 is warning customers about a critical security vulnerability affecting BIG-IP that could allow unauthenticated remote code execution.

The vulnerability, tracked as CVE-2023-46747, has a CVSS score of 9.8. The vulnerability is an authentication bypass issue and can lead to a complete compromise of an F5 system with the Traffic Management User Interface (TMUI) exposed.

To mitigate the vulnerability, F5 has made available a shell script for users of BIG-IP versions 14.1.0 and later. Certain workarounds are also available for this vulnerability. More information can be accessed here.

Trends & Reports

Cloudflare Sees Surge in Hyper-Volumetric HTTP DDoS Attacks

Summary

- Hyper-volumetric HTTP DDoS attacks have seen a sharp increase in Q3 of 2023, Cloudflare finds.

Analysis & Action

A Cloudflare report shows that the number of hyper-volumetric Hypertext Transfer Protocol (HTTP) distributed denial of service (DDoS) in the third quarter of 2023 is up almost 65%. More than 89 of the thousands detected exceeded 100 million requests per second (rps), with the largest one peaking at 201 million rps, three times the previous record.

Threat actors exploit a new vulnerability called HTTP/2 Rapid Reset (CVE-2023-44487), which has been leveraged as a zero-day since August 2023. These Rapid Reset attacks have used VM-based botnets with 5-20 million nodes to deliver significantly more power per node.

The number of HTTP DDoS attack requests has increased every quarter starting from 2023. Members can deploy Web Application Firewalls (WAF) to help filter traffic and drop malicious traffic before reaching the server. Members should also attempt to isolate their internet-facing applications to find which ones are at risk of this vulnerability. DDoS protections for layer 7 applications and layer 3 network traffic entities should also be utilized. To read the Health-ISAC threat bulletin on the topic, click here.

IoT Security Threats Highlight the Need for Zero Trust Principles

Summary

- The number of IoT attacks has increased by 400% compared to previous years, with Mirai and Gafgyt malware families accounting for 66% of attack payloads.

Analysis & Action

The number of attacks on Internet of Things (IoT) devices has increased by 400% compared to the previous year, according to Zscaler. This is a significant concern for OT (Operational Technology) security, as the malware can easily migrate within a network, potentially endangering the entire critical OT infrastructure of an organization.

The report found that cybercriminals are targeting legacy vulnerabilities, with the Mirai and Gafgyt malware families accounting for 66% of attack payloads. This is particularly relevant for the healthcare industry, which is one of the largest adopters of Internet of Things (IoT) technology, using Internet-enabled devices for patient care. These large networks of medical devices often lack endpoint security, and are notoriously difficult to patch, severely increasing the threat of a successful IoT attack on healthcare organizations.

Organizations can minimize security risks by adopting a zero-trust architecture, segmenting their networks, and utilizing continuous discovery and monitoring processes to segment devices.

Privacy, Legal & Regulatory

CISA Releases Cybersecurity Toolkit for Healthcare

Summary

- CISA has released a Cybersecurity Toolkit for Healthcare and Public Health to help healthcare organizations improve their security posture.

Analysis & Action

Cybersecurity and Infrastructure Security Agency (CISA) has released a Cybersecurity Toolkit for Healthcare and Public Health, aimed at helping cybersecurity professionals in the healthcare sector to improve the security posture of their organizations.

The toolkit includes information, guidance, and practical tools to reduce cyber risk and the likelihood of successful cyber-attacks. It includes Cyber Hygiene Services, Health Industry Cybersecurity Practices, and the HPH Sector Cybersecurity Framework Implementation Guide.

Threat actors see healthcare organizations as high-value targets due to the combination of sensitive information, including personal, financial, and medical information they store. The toolkit also intends to aid under-resourced hospitals and health facilities in improving their cyber protection in order to reduce the risk of patient care disruptions. The toolkit can be accessed here.

Health-ISAC Cyber Threat Level

On October 19, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to Yellow (Elevated). The Threat Level of Yellow (Elevated) is due to threats from concerns regarding hacktivist activity related to the conflict in the Middle East, an uptick in LinkedIn profile impersonations, MFA Bypass, QR code phishing, and the actively exploited Cisco IOS XE bug.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

Reference | References

CISA
Help Net Security
Bleeping Computer
The Hacker News
Bleeping Computer
Security Week
Bleeping Computer
Infosecurity Magazine

Tags

StripedFly, Mirth Connect, F5 BIG-IP

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP Share Threat Intel Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-

isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org