Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 5165f6bb | Oct 17, 2023, 07:13 AM

Today's Headlines:

Leading Story

- Warning: Unpatched Cisco Zero-Day Vulnerability Actively Targeted in the Wild

Data Breaches & Data Leaks

- Fairfax Healthcare Company Announces Data Breach

Cyber Crimes & Incidents

- Fake RedAlert Rocket Alert App for Israel Installs Android Spyware
- RomCom Cyber Campaign Targets Political Leaders

Vulnerabilities & Exploits

- Milesight Industrial Router Vulnerability Possibly Exploited in Attacks

Trends & Reports

- APT Trends Report Q3 2023

Privacy, Legal & Regulatory

- National Privacy Commission Launches Online Portal for PhilHealth Members to Check Data Leak

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

- Americas Hobby Exercise - October 25, 2023. Registration is available here.
- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

Warning: Unpatched Cisco Zero-Day Vulnerability Actively Targeted in the Wild

Summary

- Cisco has warned of a critical, unpatched security flaw impacting IOS XE software that is under active exploitation in the wild.

Analysis & Action

The vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege level 15 access, allowing them to gain control of the system.

The problem impacts both physical and virtual devices running Cisco IOS XE software that also has the HTTP or HTTPS server feature enabled. Cisco has attributed the attacks to presumably the same threat actor, although the adversary's exact origins are presently cloudy.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued an advisory and added the flaw to the Known Exploited Vulnerabilities (KEV) catalog.

As a mitigation, Cisco recommends disabling the HTTP server feature on internet-facing systems. Additional guidance is included in the Cisco intelligence bulletin.

Health-ISAC published a bulletin titled Cisco IOS XE Management Interface Vulnerability Actively Exploited, available for your review with additional resources.

Data Breaches & Data Leaks

Fairfax Healthcare Company Announces Data Breach

Summary

- Fairfax healthcare organization from the United States has disclosed a data breach that compromised the medical records of approximately 250,000 patients.

Analysis & Action

Fairfax Healthcare, a Virginia-based supplier of facial and dental services, has disclosed a data breach that exposed data including names, driver's licenses, Social Security numbers, health insurance, and medical history details.

There is no evidence that the exposed data has been misused, but Fairfax is notifying individuals whose personal information was contained on the encrypted systems.

Fairfax has compensated the victims of the data breach with a year of free identity protection services and has taken steps to reduce the risk of security incidents in the future.

Cyber Crimes & Incidents

Fake RedAlert Rocket Alert App for Israel Installs Android Spyware

Summary

- Israeli Android users are targeted by a malicious version of the RedAlert-Rocket Alerts that acts as spyware in the background of the infected device.

Analysis & Action

RedAlert-Rocket Alerts is a highly popular, legitimate open-source app used by Israeli citizens to receive notifications of incoming rockets. Cloudflare discovered that unknown hackers are distributing a fake version that installs spyware.

The malicious version is spread from a website that downloads an APK file on Android devices that uses the legitimate code of the real RedAlert app, so it contains all regular functionality but also accesses the victim's contacts, numbers, SMS content, installed software lists, call logs, IMEI, email, app accounts, and more.

The fake site has been taken offline, but it is likely that the threat actors will pivot to a new domain following the exposure of their operation. To distinguish between the real and laced versions of the software, review the permissions the app requests upon installation or has access to if the app has already been downloaded.

RomCom Cyber Campaign Targets Political Leaders

Summary

- Void Rabisu targeted attendees of the Women Political Leaders Summit by using a spoofed website with the espionage malware ROMCOM 4.0.

Analysis & Action

A new malware variant, ROMCOM 4.0, was used by Void Rabisu to target those who attended the August Women Political Leaders Summit 2023 conference. The attack was meant to target attendees whose goal is to further gender equality in the European Union. Void Rabisu capitalized on the invasion of Ukraine by Russia to conduct cyber espionage.

ROMCOM 4.0 is a new malware strain that has been updated from its previous version. The newly updated malware has been used to target military personnel, government employees, and politicians.

Members and their employees should be wary of Search Engine Optimization (SEO) campaigns and should ensure they both read the URL and check that it is coming from a credible source before they click on it.

Vulnerabilities & Exploits

[Milesight Industrial Router Vulnerability Possibly Exploited in Attacks]

Summary

- A vulnerability found in Chinese industrial routers holds the possibility of exploitation by threat actors.

Analysis & Action

According to VulnCheck, a vulnerability labeled CVE-2023-43261 has been found in several UR-series routers by Milesight (Ursalink). Threat actors were reported to conduct reconnaissance in the affected systems and expose private credentials.

The CVE-2023-43261 vulnerability exposes passwords used by administrators and other users, granting the threat actor access to targeted devices. UR-series routers are used in various sectors and fields, such as industrial automation, traffic lighting, smart grid assets, medical equipment, retail, and self-service kiosks. Approximately 5,500 Milesight devices were exposed to the vulnerability.

Members who use UR-series routers by Milesight are recommended to change their passwords and enable multi-factor authentication to prevent threat actors from gaining access to systems.

Trends & Reports

[APT Trends Report Q3 2023]

Summary

- Kaspersky has published its quarterly summary of advanced persistent threat activity for Q3 2023, highlighting significant events and findings.

Analysis & Action

One of the most notable findings is a new APT group that has been targeting government entities in the APAC region by compromising a specific type of secure USB drive. The group has developed sophisticated tools and techniques to carry out these attacks, which suggests that it is a highly skilled and resourceful threat actor.

Another notable finding is the increased activity of the BlindEagle APT group in South America. BlindEagle has been targeting both government entities and individuals and has shown an interest in stealing both financial data and sensitive information. The group has been cycling through various open-source remote access Trojans (RATs) in an attempt to evade detection.

The report also highlights the activities of several other APT groups, including Russian-speaking groups, Chinese-speaking groups, Spanish-speaking groups, and Middle Eastern groups.

Overall, the report shows that the APT threat landscape is constantly evolving and that threat actors are developing new tools and techniques to carry out their attacks. It is important for organizations to be aware of the latest APT threats and to take steps to protect themselves.

Privacy, Legal & Regulatory

National Privacy Commission Launches Online Portal for PhilHealth Members to Check Data Leak

Summary

- The National Privacy Commission (NPC) in the Philippines unveiled a new online portal for members to check if their data was compromised.

Analysis & Action

The NPC's new online portal is a database search tool that gives hospital members the opportunity to see if their data was exposed. After the attacks on PhilHealth by the Medusa Ransomware group, the NPC took more than 734 gigabytes of extracted data to create the new initiative. Each of these files is continuously updated to provide individuals with their information if requested.

The portal can be accessed via a PhilHealth Identification Number and, when inputted, will tell the user if their information was part of the leaked data. The NPC has focused its portal almost exclusively on the specific PhilHealth incident but plans to use the latest information regarding data leaks to update the data on file. They plan on also updating the information of patients and members of all ages.

While the NPC has not yet decided if they will continue evolving this project to account for other data breaches, the response to this specific incident sets a precedent for the protection and prevention of PHI. Members should ensure the information they store is both safe and secure and have a strategy for action in the event of a data breach.

Health-ISAC Cyber Threat Level

On September 20, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded). The Threat Level of Blue (Guarded) is due to threats from concerns regarding malvertising, rogue USB drives, Async RAT, MFA Bypass, and persistent credential stuffing/spraying.

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

Bleeping Computer
Kaspersky Labs
Heimdal Security
Security Week
Cisco Talos
The Hacker News
Backend News
Dark Reading

Tags

Milesight, RedAlert, Cisco IOS XE

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