SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 6c924ede Oct 19, 2023, 07:09 AM

Today's Headlines:

Leading Story

- Over 10,000 Cisco Devices Hacked in IOS XE Zero-Day Attacks

Data Breaches & Data Leaks

- Hacker Leaks Millions of New 23andMe Genetic Data Profiles

Cyber Crimes & Incidents

- Ukrainian Activists Hack Trigona Ransomware Gang, Wipe Servers

Vulnerabilities & Exploits

- Critical Vulnerabilities Expose Weintek HMIs to Attacks

Trends & Reports

- Cybercriminals are Targeting Plastic Surgery Offices and Patients

Privacy, Legal & Regulatory

- Five-Year-Old Privacy Goals Still Unmet by Many Federal Agencies

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

Over 10,000 Cisco Devices Hacked in IOS XE Zero-Day Attacks

Summary

- Attackers have exploited a recently disclosed critical zero-day bug to compromise and infect over 10,000 Cisco IOS XE devices with malicious implants.

Analysis & Action
It is imperative that organizations determine if systems have been compromised and take appropriate action once implants have been discovered.

On October 19, 2023, Health-ISAC provided Targeted Alerts to organizations with malicious implants detected within their environment. 24 IPs were detected with implants.

On October 18, 2023, Health-ISAC provided Targeted Alerts to organizations potentially vulnerable to the actively exploited Cisco bug.

On October 16, 2023, Health-ISAC published a Threat Bulletin titled Cisco IOS XE Management Interface Vulnerability Actively Exploited.

While a patch is not yet available, network defenders can disable the web interface and remove all management interfaces from the internet immediately as a workaround.

Data Breaches & Data Leaks

Hacker Leaks Millions of New 23andMe Genetic Data Profiles

Summary

- An additional 4.1 million genetic profiles for people in Great Britain and Germany that were stolen from 23andMe have been leaked onto a hacking forum.

Analysis & Action
This latest leak follows another one made earlier this month a threat actor leaked the stolen data of 1 million Ashkenazi Jews who used 23andMe services. The company says that only a limited number of accounts were breached but that they opted into the DNA Relative feature that allowed the threat actor to scrape millions of individuals’ data.

The amount of data that was allegedly stolen will likely result in further data leaks as the threat actor attempts to drum up enough interest to get a buyer. 23andMe says that the DNA Relatives feature turned this into a significantly larger data leak.

Lawsuits have already emerged against 23andMe with the claim that the company did not adequately protect customers' data. Members who have 23andMe accounts and have opted into the DNA Relative feature are advised to closely monitor any additional information that emerges from this story. Members are also advised to update their passwords and if possible, implement multi-factor authentication.

Cyber Crimes & Incidents

Ukrainian Activists Hack Trigona Ransomware Gang, Wipe Servers

Summary

- Ukrainian hacktivists have breached the servers of the Trigona ransomware group.

Analysis & Action

The Ukrainian Cyber Alliance is a pro-Ukrainian hacktivist outfit. They claimed to have breached Trigona ransomware group's servers, and exfiltrated copies of all data before deleting everything in the servers. Some analysts believe there may have been decryption keys in the data exfiltrated.

The hacktivist group was able to gain access to the servers through a public exploit of CVE-2023-22515, a remote privilege escalation vulnerability affecting Confluence Data Center and Server software. The group has agreed to release any decryption keys if they are found within the data leaks.

Trigona ransomware represents a unique case of hacktivism taking down a ransomware group, as opposed to the coordinated law enforcement operations that resulted in the seizure of ransomware infrastructure in the past. As hacktivists become more and more advanced in the search for internet stardom, the types of attacks executed by hacktivists are likely to become increasingly advanced, with significant investment into new capabilities being made.

Vulnerabilities & Exploits

Critical Vulnerabilities Expose Weintek HMIs to Attacks

Summary

- Critical manufacturing organizations are at risk of cyberattacks from Weintek's human-machine interface (HMI) vulnerabilities being exposed.

Analysis & Action

The discovery of three vulnerabilities within Taiwan-based Weintek's HMI has opened risks of exploitation for manufacturing organizations, some of which are linked to critical infrastructure. These flaws pose a critical risk to the security of critical manufacturing organizations, as the threat actors can completely take control of an HMI with these vulnerabilities unpatched.

Through these vulnerabilities, threat actors can bypass the authentication process and gain access to the systems or execute commands remotely. The threat actors can execute arbitrary commands with access to the HMI's password

Members who utilize Weintek are encouraged to look over the technical details for each of the vulnerabilities provided by TXOne and are recommended to update their software to decrease the chances of threat actors exploiting vulnerabilities.

Trends & Reports

Cybercriminals are Targeting Plastic Surgery Offices and Patients

Summary

- The FBI is warning the public about cybercriminals who target plastic surgery offices, surgeons, and patients to harvest personally identifiable information and sensitive medical records, including sensitive photographs in some instances.

Analysis & Action

Cybercriminals use phishing to deploy malware to plastic surgery offices. Once successful, cybercriminals harvest electronically protected health information (ePHI), which includes sensitive information and photographs.

Next, cybercriminals use open-source information, including social media, and social engineering techniques, to enhance the harvested ePHI data of plastic surgery patients.

Lastly, cybercriminals contact plastic surgeons and their patients via social media accounts, emails, text messages, or messaging apps, and ask for payment to prevent sharing of their ePHI.

Privacy, Legal & Regulatory

Five-Year-Old Privacy Goals Still Unmet by Many Federal Agencies

Summary

- Numerous federal agencies have failed to meet privacy goals set in place five years ago.

Analysis & Action

The State Department, Department of Housing and Urban Development, the National Aeronautics and Space Administration (NASA), as well as others, are yet to meet the privacy goals set by the National Institute of Standards and Technology (NIST) five years ago. These goals highlight the importance of integrating privacy into risk management systems, which numerous federal agencies have yet to do.

More than a year ago, the Government Accountability Office (GAO) found that 14 agencies failed to meet these privacy goals, and suggested there be challenges in the federal government to privacy management. This caused a lot of concern regarding the government’s lack of preparedness to handle the growth of the artificial intelligence field.

While these are the goals of federal agencies, members should ensure that they have integrated privacy into their risk management systems.

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
Bleeping Computer
Security Week
txone
SC Magazine
Bleeping Computer
IC3

Tags

23andMe, Weintek HMIs, Cisco IOS, Cisco

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