Health-ISAC™

Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : 3232fae8 Oct 03, 2023, 07:11 AM

Today’s Headlines:

Leading Story

- Security Researchers Believe Mass Exploitation Attempts Against WS_FTP Have Begun

Data Breaches & Data Leaks

- Hackers Steal User Database from European Telecommunications Standards Body
- DHS Investigating Extent of Johnson Controls Security Breach

Cyber Crimes & Incidents

- AWS Stirs the MadPot – Busting Bot Baddies and Eastern Espionage Since 2010

Vulnerabilities & Exploits

- Cisco Warns of Attempted Exploitation of Zero-Day in VPN Software

Trends & Reports

- FBI Warns of Surge in Phantom Hacker Scams Impacting Elderly

Privacy, Legal & Regulatory

- Nothing to Report.

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

Security Researchers Believe Mass Exploitation Attempts Against WS_FTP Have Begun

Summary

- Security researchers have spotted what they believe to be a possible mass exploitation of vulnerabilities in Progress Software’s WS_FTP Server.

Analysis

Rapid 7 has noted evidence of exploitation of one or more of eight vulnerabilities in WS_FTP that Progress released fixes for on Wednesday.

Researchers have noted a single Burpsuite domain used in every exploit attempt so far, leading to the idea that a single threat actor is responsible for the attempts.

Members are advised to update to the latest version of WS_FTP as soon as possible to address the vulnerabilities in the previous version. Members who are using WS_FTP with the Ad Hoc Transfer module are encouraged to either disable or remove the module.

Health-ISAC has previously distributed a vulnerability bulletin regarding the critical vulnerability, which can be accessed here.

Data Breaches & Data Leaks

Hackers Steal User Database From European Telecommunications Standards Body

Summary

- A database identifying users of the European Telecommunications Standards Institute has been stolen by unknown threat actors.

Analysis
According to The Record, unknown threat actors have stolen data identifying the users of the European Telecommunications Standards Institute (ETSI).

Current sources say that the motive is unclear, and whether the attack was financially motivated or motivated through espionage remains unknown. While it is still not concluded if the credentials of users were stolen, members were asked to create new logins and passwords, eliminating the possibility for hackers to go back into the member systems.

The vulnerability has been fixed with the help of France's cybersecurity agency, the ANSSI. The ETSI declined to clarify if the vulnerability the threat actors targeted was a known vulnerability or a zero-day. Members are encouraged to undertake additional security measures to strengthen IT security procedures and prevent vulnerabilities from being exploited by threat actors.

DHS Investigating Extent of Johnson Controls Security Breach

Summary

- A cyberattack on Johnson Controls has potentially given attackers a physical security map of many Department of Homeland Security (DHS) facilities.

Analysis & Action
Alarm and building automation company, Johnson Controls, was recently the victim of a cyberattack. They hold classified contracts for DHS that layout both floorplans and the physical security of DHS facilities. While it is not known the extent of the information the attackers have obtained, Johnson Controls and DHS are working under the assumption that they have access to these floor plans and security information.

The attack on Johnson Controls' servers has severe impacts that go well beyond the scope of the information of one company being leaked. In this instance, that information possesses vital intel on DHS facilities and their security, which can aid actors in conducting an attack. While the actors responsible for the attack have not yet been named, an external group of cybersecurity experts has been brought in to assist in the recovery from the incident.

Members who utilize Johnson Controls should be made aware of the possibility that their physical security maps and other physical security information have been breached.

Cyber Crimes & Incidents

AWS Stirs the MadPot – Busting Bot Baddies and Eastern Espionage Since 2010

Summary

- Amazon Web Services unveiled MadPot, a threat-intelligence tool to thwart Chinese and Russian spies, protecting critical infrastructure.

Analysis & Action

Amazon Web Services (AWS) new MadPot is a new part of their honeypot system that has been in development for thirteen years.

It is comprised of thousands of sensors that monitor any attempts by criminals or unwanted nation-state actors to connect with AWS decoys. AWS has said that more than 100 million potential threats are spotted each day by MadPot. One of its most important successes was preventing Chinese spies from gaining critical intel on US infrastructure networks. MadPot also contributed to the Five Eyes' advisory regarding one of Beijing's cyber-espionage gangs, Volt Typhoon, and eventually led to the federal government being able to take down their command-and-control (C2) servers, significantly delaying future attacks.

Systems like MadPot are continuously being developed by companies to prevent cybercriminals from gaining access to critical infrastructure networks.

Vulnerabilities & Exploits

Cisco Warns of Attempted Exploitation of Zero-Day in VPN Software

Summary

- Threat actors are attempting to exploit a vulnerability found in Cisco's VPN products.

Analysis

According to The Record, threat actors have attempted to exploit the vulnerabilities affecting the Cisco Group Encrypted Transport VPN (GET VPN).

Success in GET VPN's exploitation could result in the threat actor gaining full control of the system or cause the affected system to reload by executing an arbitrary code. Cisco reports that both means of exploitation require previous infiltration of the systems.

Members are encouraged to closely monitor systems for potential vulnerabilities and update security measures to avoid exploitation of private information.

Trends & Reports

FBI Warns of Surge in Phantom Hacker Scams Impacting Elderly

Summary

- A recent public service announcement from the FBI warns of increasing phantom hacker scams that target senior citizens across the US.

Analysis & Action

Threat actors initiate contact with victims in three steps. First, they are pretending to be bank representatives contacting individuals and falsely claiming their accounts have been the victim of a hacking attempt and should anticipate a call from their bank.

The second call advises the victim to transfer their funds to a secure account, which the threat actor controls. A third call claims to be from a representative of the US government to persuade suspicious victims to transfer their funds to the new account.

The FBI is advising individuals vulnerable to scams against engaging in unsolicited pop-ups, links sent through text messages, email attachments, or calling a number provided through these means.

Privacy, Legal & Regulatory

Nothing to Report.

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

The Record
Bleeping Computer
The Register
The Register
Campus Safety Magazine
The Record

Tags

MadPot, WS_FTP, DHS, AWS, Progress

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