Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 485da4e3 | Oct 15, 2024, 07:58 AM

Today's Headlines:

Leading Story

- Critical Veeam Vulnerability Exploited to Spread Akira and Fog Ransomware

Data Breaches & Data Leaks

- Gryphon Healthcare, Tri-City Medical Center Disclose Significant Data Breaches
- Cisco Investigates Breach After Stolen Data for Sale on Hacking Forum

Cyber Crimes & Incidents

- China Accuses U.S. of Fabricating Volt Typhoon to Hide Its Own Hacking Campaigns

Vulnerabilities & Exploits

- Chinese State Hackers Main Suspect in Recent Ivanti CSA Zero-Day Attacks
- WordPress Plugin Jetpack Patches Major Vulnerability Affecting 27 Million Sites

Trends & Reports

- PCs Are Poised To Fall off the Windows 10 Update Cliff One Year From Today

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – October 29, 2024, 12:00-01:00 PM ET

    - European – October 30, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – November 14, 2024 at 11:30 AM ET
- European Summit, Athens, Greece - October 15-17, 2024
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

Critical Veeam Vulnerability Exploited to Spread Akira and Fog Ransomware

Summary

- Threat actors are exploiting critical RCE flaw CVE-2024-40711 in the Veeam Backup & Replication solution.

Analysis & Action

Cybersecurity vendor Sophos has reported a series of attacks leveraging compromised VPN credentials and CVE-2024-40711 to deploy Akira and Fog ransomware.

CVE-2024-40711 is a critical vulnerability affecting the Veeam Backup & Replication solution. The flaw has a CVSS score of 9.8 and allows for unauthenticated remote code execution. In the observed attack, threat actors accessed targets using compromised VPN gateways without adequate authentication controls and exploited the flaw on the URI /trigger on port 8000. The Fog ransomware deployment involved dropping the ransomware to an unprotected Hyper-V server and using the rclone utility to exfiltrate data.

Veeam Backup & Replication version 12.2 addressed the flaw. Health-ISAC recommends immediately patching the vulnerability and continuously monitoring systems for any sign of suspicious activity.

Data Breaches & Data Leaks

Gryphon Healthcare, Tri-City Medical Center Disclose Significant Data Breaches

Summary

- Gryphon Healthcare and Tri-City Medical Center reported data breaches together affecting a total greater than 500,000 patients.

Analysis & Action

The Houston-based medical billing service provider, Gryphon Healthcare, disclosed a data breach affecting 393,358 individuals. The breach occurred on August 13, 2024, due to a security incident involving a partner. Sensitive patient information, including names, addresses, Social Security numbers, and medical records, was compromised.

On the other hand, Tri-City Medical Center revealed a data breach that affected 108,149 individuals. The breach occurred in November 2023 due to a cyberattack that disrupted systems and exposed data. An investigation completed in September 2024 determined that personal information, including names and other identifiers, was compromised during the attack.

Health-ISAC recommends that organizations implement comprehensive security measures to help prevent successful intrusions that negatively impact the confidentiality, integrity, and availability of critical infrastructure or patients' personal information.

Cisco Investigates Breach After Stolen Data for Sale on Hacking Forum

Summary

- Cisco is currently investigating claims about a potential breach by the threat actor IntelBroker.

Analysis & Action

Cisco is investigating claims of a breach following a hacking forum where a threat actor, IntelBroker, claimed to have stolen data from Cisco. The company has launched an investigation to assess the claim and is currently investigating the matter.

IntelBroker, along with two others, claims to have breached Cisco on June 10th, 2024, and stole a large amount of developer data. The threat actor has shared data samples that were presumably meant to prove the legitimacy of the breach. The leaked data included a database, customer

information, various customer documentation, and screenshots of customer management portals. The data was allegedly stolen from a third-party managed services provider for DevOps and software development.

Health-ISAC recommends staying vigilant and implementing rigorous security controls, including network segmentation, to minimize the impact of a successful attack.

Cyber Crimes & Incidents

China Accuses U.S. of Fabricating Volt Typhoon to Hide Its Own Hacking Campaigns

Summary

- China's National Computer Virus Emergency Response Center (CVERC) has repeatedly denied the existence of the Volt Typhoon threat actor.

Analysis & Action

The CVERC accuses the U.S. of conducting cyber espionage activities against China and other countries and of using false flag operations to conceal its own malicious cyber attacks.

The CVERC has not provided any concrete evidence to support its claims and has instead accused the U.S. of using various tactics to mislead investigators and frame China.

The report concludes by calling for international collaboration in cybersecurity and for companies and research institutions to focus on counter-cyber threat technology research and better products and services for users.

Vulnerabilities & Exploits

Chinese State Hackers Main Suspect in Recent Ivanti CSA Zero-Day Attacks

Summary

- Chinese state-sponsored threat actors are assessed to be behind recent exploitation attacks against zero-days affecting Ivanti Cloud Services Application (CSA) products.

Analysis & Action

Recently, Ivaniti has disclosed that several CSA zero-days have been chained together to exploit a limited number of vulnerable customer systems. The main vulnerability tracked as CVE-2024-8190, allows remote code execution; however, exploitation of the security flaw requires elevated privileges in which threat actors are chaining together other bugs to accomplish. These vulnerabilities include flaws such as CVE-2024-8963, CVE-2024-9379, and CVE-2024-9380.

Once the Ivanti CSA product has been compromised, the threat actor has been observed conducting lateral movement, deploying web shells, collecting information, conducting scanning and brute-force attacks, and abusing the appliance for proxying traffic, among other nefarious operations.

According to investigations by Ivanti, the observed activity is likely that of a nation-state adversary, but it has not identified the threat group. However, a researcher noted an IP released by Ivanti as an indicator of compromise previously attributed to UNC4841, which is a China-linked threat group. Health-ISAC recommends immediately patching vulnerable Ivanti CSA products to prevent exposure to potential exploitation attacks and the compromise of sensitive data or disruptions to critical infrastructure.

WordPress Plugin Jetpack Patches Major Vulnerability Affecting 27 Million Sites

Summary

- Security updates have been released by Jetpack Wordpress plugin maintainers for a critical vulnerability affecting several sites.

Analysis & Action

The maintainers of the Jetpack WordPress plugin released a security update to address a critical vulnerability that could allow logged-in users to access forms submitted by others on a site. Jetpack is an all-in-one plugin that provides a suite of tools helping users to improve site safety, performance, and traffic growth.

The vulnerability was identified by Jetpack during an internal security audit affecting versions up to 3.9.9 and resides in the Contact Form feature. The security flaw could ultimately be used by any

logged in user on a site to read forms submitted by visitors on the site.

Jetpack has worked closely with WordPress to automatically update the plugin to a safe version on installed sites. The security flaw has been addressed in several different iterations of Jetpack. Due to the disclosure of the vulnerability, the likelihood of exploitation has increased. Health-ISAC recommends that users ensure their Jetpack WordPress plugins are always up-to-date to maintain optimal performance, security, and compatibility.

Trends & Reports

PCs Are Poised To Fall off the Windows 10 Update Cliff One Year From Today

Summary

- Microsoft will stop releasing security updates for Windows 10 PCs on October 14, 2025.

Analysis & Action

While organizations and individuals can still pay for extended support for three more years, many Windows 10 PCs will no longer be supported.

This is a significant change compared to previous Windows operating systems, as the time window between replacement and retirement is shorter and a larger percentage of the user base is still actively using Windows 10.

Many Windows 10 PCs cannot be updated to Windows 11 due to system requirements. As a result, users will need to consider alternatives such as upgrading to an unsupported Windows 11 installation, using a different operating system like Linux or ChromeOS Flex, or purchasing a new PC.

Privacy, Legal & Regulatory

Nothing to Report.

Health-ISAC Cyber Threat Level

On September 19, 2024, 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:

The Threat Level of Blue (Guarded) is due to threats from DPRK IT fraud, elections-induced cyber activity, potential repercussions of recent activity in the Middle East, potential Ivanti Endpoint Manager exploitation, and ongoing observances of infostealer's logs being posted on Telegram.

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.

Report Source(s)

Health-ISAC

Incident Date

Oct 15, 2024, 11:59 PM

Reference | References

The Hacker News
Security Week
Bleeping Computer
Security Week
The Hacker News
Ars Technica
The Hacker News

Tags

Breach Victims, VMware NSX Vulnerabilities, Linear eMerge E3 Systems Flaw, Internet of Healthcare Things (IoHT), Data Breaches

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 HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org