Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : fd6d3734 | Oct 05, 2023, 08:49 AM

Today's Headlines:

Leading Story

- Zero-Day Privilege Escalation in Confluence Server and Data Center

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

- Researchers Warn of 100,000 Industrial Control Systems Exposed Online
- Mozilla Warns of Fake Thunderbird Downloads Delivering Ransomware

Vulnerabilities & Exploits

- Cisco Fixes Hard-Coded Root Credentials in Emergency Responder
- Looney Tunables Bug Opens Millions of Linux Systems to Root Takeover

Trends & Reports

- Ransomware Double-Extortion Attacks Increased 72%

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

Zero-Day Privilege Escalation in Confluence Server and Data Center

Summary

- Atlassian has released fixes to contain an actively exploited critical zero-day flaw impacting publicly accessible Confluence Data Center and Server instances.

Analysis & Action

Atlassian published a security advisory on CVE-2023-22515, a critical privilege escalation vulnerability affecting on-premises instances of Confluence Server and Confluence Data Center, which has been exploited in attacks. Health-ISAC has distributed a bulletin in relation to this vulnerability that can be viewed here.

Atlassian does not specify the root cause of the vulnerability or where exactly the flaw resides in Confluence implementations, though the indicators of compromise include mention of the /setup/* endpoints. Tracked as CVE-2023-22515 (CVSS 10), this critical privilege escalation flaw affects Confluence Data Center and Server 8.0.0 and later and is described as being remotely exploitable in low-complexity attacks that don't require user interaction.

Besides upgrading and applying mitigation measures, Atlassian also urges customers to shut down impacted instances or isolate them from Internet access if immediate patching isn't possible.

Data Breaches & Data Leaks

- Nothing to Report

Cyber Crimes & Incidents

Researchers Warn of 100,000 Industrial Control Systems Exposed Online

Summary

- Around 100,000 Industrial Control Systems (ICS) in critical infrastructure sectors across 96 different countries were found to be exposed online.

Analysis & Action

About 100,000 ICSs were found on the public web. These belong to critical systems such as power grids, traffic light systems, security, and water systems. These exposed systems run the risk of threat actors scanning for vulnerabilities and gaining unauthorized access to them.

BitSight alerted many to the problem, which impacted many of the Fortune 1000 companies around the world. While it is not known how many of the 100,000 exposed ICSs are vulnerable, possible exploitation still poses a unique threat to the healthcare industry as relies on other sectors like transportation, the grid, water, and others to be fully functional.

Members are advised to make sure that there are no public-facing industrial control systems or supervisory control and data acquisition (SCADA) panels to avoid possible attacks.

Mozilla Warns of Fake Thunderbird Downloads Delivering Ransomware

Summary

- Malicious websites offering fake Mozilla Thunderbird downloads threaten the data security of unsuspecting users.

Analysis & Action

According to Security Week, the Snatch ransomware group has been using malicious websites to offer fake Thunderbird downloads to users. Snatch has been known to leak personal data and internal operations of their victims.

The Snatch ransomware group delivers their malware through malicious Google ads pretending to be legitimate ads for popular applications such as Adobe Reader, Discord, Microsoft Teams, and Mozilla Thunderbird. Mozilla is currently trying to take down the websites that offer fake Thunderbird downloads.

Members are encouraged to verify the sources of their downloads to prevent malware and ransomware attacks and be on the lookout for suspicious websites offering application downloads.

Vulnerabilities & Exploits

Cisco Fixes Hard-Coded Root Credentials in Emergency Responder

Summary

- Cisco released security updates for a Cisco Emergency Responder (CER) vulnerability allowing threat actors access to unpatched systems using hard-coded credentials.

Analysis & Action

The flaw is tracked as CVE-2023-20101 and allows unauthenticated attackers to access a targeted device using the root account which had default static

credentials that could not be removed or modified.

At the current moment, Its Product Security Incident Response Team (PSIRT) has not discovered any information regarding public disclosures or malicious exploitation related to the CVE-2023-20101 vulnerability.

There are no workarounds to mitigate the security flaw temporarily, Cisco advises admins to update vulnerable installations as soon as possible. Health-ISAC recommends that members who utilize CER update their system to avoid any potential exploitation and to monitor their systems for any unauthorized access.

Looney Tunables Bug Opens Millions of Linux Systems to Root Takeover

Summary

- A bug found in many major Linux distributions grants root privileges to threat actors.

Analysis & Action

A newly discovered buffer overflow vulnerability in millions of Linux systems can grant root privileges to threat actors. Major Linux distros such as Fedora, Ubuntu, and Debian are reported to be at the most risk regarding the bug.

The bug is mainly found in GNU C Library (glibc) and poses a major risk of unauthorized data access, system altercations, and potential data theft in millions of Linux systems. Risks are also present to consumer gear, such as drones, robots, and smart factories.

Members are advised to update their Linux distributions as soon as possible to patch up any vulnerabilities and undertake additional security measures to keep systems secure.

Trends & Reports

Ransomware Double-Extortion Attacks Increased 72%

Summary

- Double-extortion attacks have increased 72% by quarter while detections on endpoints have declined 72% by year.

Analysis & Action

A report conducted by WatchGuard found and analyzed different malware and network security trends. The report found that 95% of malware hides behind encrypted SSL/TLS connections used by websites.

Double-extortion attacks have sharply increased by around 72%. The report finds that one of the possible reasons for this is that there are around 13 new extortion groups that have been tracked by WatchGuard. While these double-extortion attacks have increased overall, the number of attacks that are registering as ransomware detections on endpoints has declined by around 21% from Q1 to Q2 of 2023 and 72% from the entire year.

Members should continue to protect PHI they have access to in order to prevent cybercriminals encrypting the data and threatening to publish and sell it. Multi-factor authentication (MFA) and secure Wi-Fi connections are both important practices to put in place to prevent PHI from being stolen. To view the WatchGuard report, click here.

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 Hacker News
Enumerating Subdomains with Common Crawl PowerPoint Presentation
Bleeping Computer
Security Week
Bleeping Computer
Dark Reading
Security Magazine

Tags

CVE-2023-22515, Snatch, mozilla, Cisco, Linux, ICS

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