Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : c43d741a | Oct 04, 2023, 07:08 AM

Today's Headlines:

Leading Story

- Qualcomm Releases Patch for 3 Zero-Days Under Active Exploitation

Data Breaches & Data Leaks

- Microsoft Warns of Cyber Attacks Attempting to Breach Cloud via SQL Server Instance

Cyber Crimes & Incidents

- Critical TorchServe Flaws Could Expose AI Infrastructure of Major Companies
- EvilProxy Uses indeed.com Open Redirect for Microsoft 365 Phishing

Vulnerabilities & Exploits

- North Korea Poses as Meta to Deploy Complex Backdoor at Aerospace Org
- Over 3 Dozen Data-Stealing Malicious npm Packages Found Targeting Developers

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- FDA Cyber Mandates for Medical Devices Goes into Effect

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

Qualcomm Releases Patch for 3 Zero-Days Under Active Exploitation

Summary

- Qualcomm is warning of three zero-day vulnerabilities in its GPU and Compute DSP drivers that hackers are actively exploiting in attacks.

Analysis & Action

Google's Threat Analysis Group (TAG) and Project Zero teams identified vulnerabilities under limited, targeted exploitation.

Qualcomm released security updates that address the issues in its Adreno GPU and Compute DSP drivers along with a strong recommendation to deploy security updates as soon as possible.

Review Qualcomm's October 2023 Security Bulletin with additional details including affected chipsets, CVSS scores, and links to publicly available code for more insight.

Data Breaches & Data Leaks

Microsoft Warns of Cyber Attacks Attempting to Breach Cloud via SQL Server Instance

Summary

- Microsoft has shared details related to a new campaign in which attackers unsuccessfully attempted to move laterally to a cloud environment through a SQL server instance.

Analysis & Action

Microsoft shared details related to a new campaign observed indicating attackers initially exploited a SQL injection vulnerability to gain access and elevated permissions on a SQL server instance deployed in Azure.

The attackers then attempted to move laterally within the cloud infrastructure by abusing the server's cloud identity.

Microsoft stated the attack was unsuccessful and shared details of the attack to assist network defenders in managing authentication identities associated with cloud resources and services.

Cyber Crimes & Incidents

Critical TorchServe Flaws Could Expose AI Infrastructure of Major Companies

Summary

- A series of critical vulnerabilities impacting TorchServe could allow threat actors to take control of servers that are part of the artificial intelligence (AI) infrastructure of multiple companies.

Analysis & Action

TorchServe is an open-source package in PyTorch which is currently part of the Linux Foundation and is used by major companies such as Google, Intel, and Microsoft. The vulnerabilities discovered could compromise the AI infrastructure of the organization and allow threat actors to gain initial access and execute malicious code on the targeted PyTorch server with lateral movement.

Oligo researchers identified three vulnerabilities in TouchServe, referring to the attack as ShellTorch. Only one CVE identifier has been assigned: CVE-2023-43654. One of the vulnerabilities is a default misconfiguration that results in TorchServe management interface being exposed to remote access without authentication while the other two vulnerabilities can be exploited for remote code execution through server-side request forgery (SSRF) and through unsafe deserialization.

Versions 0.3.0 through 0.8.1 are impacted by these vulnerabilities. Members who utilize this tool should update it to version 0.8.2 to patch some of the flaws.

EvilProxy Uses indeed.com Open Redirect for Microsoft 365 Phishing

Summary

- Executives at numerous organizations are having their Microsoft 365 accounts targeted by a threat actor using EvilProxy abusing open redirects from job listings on Indeed.

Analysis & Action

EvilProxy, a phishing service that collects session cookies to bypass multi-factor authentication (MFA) mechanisms, is being used in a recently uncovered phishing campaign that is targeting the Microsoft 365 accounts of executives in organizations who have put out job listings on Indeed.

Targets are receiving emails with an Indeed link that passes the eye test for legitimacy but takes the user to a phishing site that acts as a reverse proxy for the Microsoft login page. The link can bypass email security measures because it comes from a trustworthy party. EvilProxy is the platform that uses these reverse proxies to communicate and relay user delays between the target and the real server is being used. The user logs into their account via the EvilProxy server, it captures their authentication cookies, giving the hackers full access to the victim's account.

The practice of combining open redirects with the use of a reverse proxy kit is growing, and members should be aware of the risks that come with it. Members are encouraged to only click on links that come from trusted addresses and link to familiar sites.

Vulnerabilities & Exploits

North Korea Poses As Meta to Deploy Complex Backdoor at Aerospace Org

Summary

- North Korean state-sponsored threat actor, Lazarus Group, used their new malware, LightlessCan in a cyberattack against a Spanish aerospace company.

Analysis & Action

Lazarus Group posed as Meta recruiters and messaged members of a Spanish aerospace company through LinkedIn. Employees were given basic coding problems to test their proficiency in C++, but these tests also held malicious executables that downloaded payloads onto the employee's system when they solved the problems.

LightlessCan has the capacity to execute native Windows commands within the RAT, making it much more advanced than BlindingCan. LightlessCan supports more than 68 unique commands, many of which can mimic Windows commands which makes the payload difficult to monitor and detect. LightlessCan payloads are encrypted and can only be decrypted using a key that is specific to the compromised machine.

Lazarus Group has had a history of using malware to target healthcare entities which makes it possible that LightlessCan could be used in a supply chain attack against healthcare in the future, similar to what was seen in the 3CX attacks. It is recommended that members remind their employees to watch for LinkedIn scams and have endpoint detection and response (EDR) solutions or similar anti-malware technology.

Over 3 Dozen Data-Stealing Malicious npm Packages Found Targeting Developers

Summary

- According to cybersecurity researchers, approximately 36 phony software packages have been discovered containing information-steal malware.

Analysis & Action

npm is the world's largest open-source software registry. Developers use its software packages to assist in writing JavaScript applications. According to Fortinet, there are nearly 36 counterfeit packages that contain information-stealing malware meant to steal sensitive data from developer machines.

The malware contained within these fraudulent npm packages has been observed targeting sensitive areas of the developer's machine, such as SSH keys, Kubernetes configurations, and system metadata. The malware was also observed extracting source code samples, credentials, and confidential directories to obtain intellectual property, and then uploading it to an FTP server.

According to ENISA, the cybersecurity agency of the European Union, software supply chain attacks such as these malicious npm packages are likely to be the most severe cyber risk in 2030. In the meantime, members are advised to validate software packages prior to integration into products and create thorough software bills of materials (SBOMs) for new projects.

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

FDA Cyber Mandates for Medical Devices Goes into Effect

Summary

- The Biden administration is pushing the manufacturers of medical devices to take on greater responsibility to ensure that they are secure.

Analysis & Action

New regulations from the Food and Drug Administration (FDA) aim to make it more difficult to hack into medical devices by requiring vendors to beef up the security features of their products.

The regulations, which went into effect on October 2, 2023, require vendors to:

- Create processes to find and mitigate vulnerabilities
- Create a software bill of materials

- Have a plan in place to address vulnerabilities for products after they have been sold

The FDA also has the authority to refuse to accept devices that do not meet its cybersecurity guidelines.

The new regulations are a significant step forward in protecting medical devices from cyberattacks. However, some argue that the FDA could be more aggressive in policing the industry, given the critical need to protect systems that care for human life.

The regulations are part of a broader push by the Biden administration to sharpen cybersecurity regulations across the private sector.

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

Qualcomm
Security Week
Dark Reading
Cyberscoop
The Hacker News
The Hacker News
Bleeping Computer
The Hacker News

Tags

Meta, FDA, Npm, Qualcomm, Microsoft

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