Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:GREEN** **Alert Id: 56aa8160** **2022-10-31 12:50:17**

Today’s Headlines:

Leading Story

- Exploit Released for Critical VMware RCE Vulnerability, Patch Now

Data Breaches & Data Leaks

- Twilio Reveals Another Breach from the Same Hackers Behind the August Hack

Cyber Crimes & Incidents

- Unofficial Patch Released for New Actively Exploited Windows MotW Vulnerability

Vulnerabilities & Exploits

- GitHub Repojacking Bug Could Have Allowed Attackers to Takeover Other Users' Repositories
- Active Exploitation of a Zero-day Vulnerability in Chrome Web Browser

Trends & Reports

- MDIC Releases Medical Device Security Maturity Benchmarking Report

Privacy, Legal & Regulatory

- Europe Prepares to Rewrite the Rules of the Internet

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – November 29, 2022, 12:00 PM Eastern

Leading Story

Exploit Released for Critical VMware RCE Vulnerability, Patch Now

Summary

- Proof-of-concept exploit code is now available for a pre-authentication remote code execution (RCE) vulnerability allowing attackers to execute arbitrary code remotely with root privileges on unpatched Cloud Foundation and NSX Manager appliances.

Analysis & Action

The flaw, CVE-2021-39144, is in the XStream open-source library used by the two VMware products and was assigned a CVSSv3 base score of 9.8/10 by VMware.

Unauthenticated threat actors can exploit it remotely in low-complexity attacks that will not require user interaction.

VMware released security updates to address the CVE-2021-39144 flaw.

Data Breaches & Data Leaks

Twilio Reveals Another Breach from the Same Hackers Behind the August Hack

Summary

- Communication services provider Twilio experienced a security incident in August, 2022 that was similar to another incident in June, 2022.

Analysis & Action

The unauthorized access resulted in compromised customer information. In the June incident, a Twilio employee was socially engineered through voice phishing to provide their credentials, and the malicious actor was able to access customer contact information for a limited number of customers.

Details of the second breach come as Twilio noted the threat actors accessed the data of 209 customers, up from 163 it reported on August 24.

The attack against Twilio has been attributed to a hacking group tracked by Group-IB and Okta under the names 0ktapus and Scatter Swine, and is part of a broader campaign against software, telecom, financial, and education companies.

Cyber Crimes & Incidents

Unofficial Patch Released for New Actively Exploited Windows MotW Vulnerability

Summary

- An unofficial patch has been made available for an actively exploited security flaw in Microsoft Windows that makes it possible for files signed with malformed signatures to sneak past Mark-of-the-Web (MotW) protections.

Analysis & Action

While files downloaded from the internet in Windows are tagged with a MotW flag to prevent unauthorized actions, it has since been found that corrupt Authenticode signatures can be used to allow the execution of arbitrary executables without any SmartScreen warning.

Authenticode is a Microsoft code-signing technology that authenticates the identity of the publisher of a particular piece of software and verifies whether the software was tampered with after it was signed and published.

If the file has a malformed Authenticode signature, the SmartScreen and/or file-open warning dialog will be skipped. The zero-day bug is the result of SmartScreen returning an exception when parsing the malformed signature, which is incorrectly interpreted as a decision to run the program rather than trigger a warning.

Vulnerabilities & Exploits

GitHub Repojacking Bug Could Have Allowed Attackers to Takeover Other Users' Repositories

Summary

- The Cloud-based repository hosting service GitHub has addressed a high-severity security flaw that could have been exploited to create malicious repositories and mount supply chain attacks.

Analysis & Action
The RepoJacking technique, disclosed by Checkmarx, entails a bypass of a protection mechanism called popular repository namespace retirement, which aims to prevent developers from pulling unsafe repositories with the same name.

RepoJacking occurs when a creator of a repository opts to change the username, potentially enabling a threat actor to claim the od username and publish a rogue repository with the same in an attempt to trick users into downloading them.

A successful exploitation could have effectively allowed attackers to push poisoned repositories, putting renamed usernames at risk of being a victim of supply chain attacks.

Active Exploitation of a Zero-day Vulnerability in Chrome Web Browser

Summary

- Google released a patch for an actively exploited zero-day vulnerability today.

Analysis & Action
Google just released a patch to Google chrome that eliminates an actively exploited zero-day vulnerability tracked as CVE-2022-3723. This vulnerability allowed attackers to access parts of the browser memory leading to the jeopardization of other web apps within chrome.

In addition to the potential to obtain credentials stored within Chrome, this zero-day also allowed for remote code execution (RCE) and had the ability to crash web applications.

The update to fix this zero-day is out now, however the same update will be released for other Chromium-based browsers soon. Health-ISAC recommends updating Google Chrome and any other chromium-based browsers such as Microsoft Edge, Vivaldi, Opera, Chromium, and Brave as soon as the update becomes available.

Trends & Reports

MDIC Releases Medical Device Security Maturity Benchmarking Report

Summary

- The medical device security maturity benchmarking report provides a baseline for assessing the current state of device cybersecurity efforts.

Analysis & Action
As the concern around medical device security continues, the need for industry-wide standards has provided numerous hurdles for the sector and could pose patient safety.

To address these challenges and gain insight into the current state of the industry, the Medical Device Innovation Consortium (MDIC) released its first medical device security maturity benchmarking tool and report based on survey responses from 17 medical device manufacturers (MDMs).

The findings curated by Booz Allen Hamilton and MDIC found that the industry as a whole has a low level of cybersecurity maturity, especially concerning Design Control. The full report can be found here.

Privacy, Legal & Regulatory

Europe Prepares to Rewrite the Rules of the Internet

Summary

- EU hopes DMA will force Big Tech platforms to break open their walled gardens.

Analysis & Action

On November 1, the European Union's Digital Markets Act, or DMA, comes into force, starting the clock on a process expected to force Amazon, Google, and Meta to make their platforms more open and interoperable in 2023.

Like the EU's digital privacy law, GDPR, the DMA is expected to lead to changes in how tech platforms serve people beyond the EU's 400 million Internet users, because some details of compliance will be more easily implemented globally.

Tech companies will also soon have to grapple with a second sweeping EU law, the Digital Services Act, which requires risk assessments of some algorithms and disclosures about automated decision-making.

Health-ISAC Cyber Threat Level

On October 20, 2022, 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) was chosen in response to ongoing Qbot activity, fraudulent Help Desk activity, ongoing ransomware attacks, observed credential phishing, and foreign policy quandaries amid midterm elections.

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(s): Bleeping Computer, The Hacker News, The Hacker News, The Hacker News, CSA, Health IT Security, Ars Technica

Tags: VM Ware, Netwrix, Google Zero Day, Daily Cyber Headlines, GitHub repo, European Union (EU), Medical Devices, DCH

TLP:GREEN: Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

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