Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : e689aff6 | Oct 31, 2023, 07:54 AM

Today's Headlines:

Leading Story

- ServiceNow Data Exposure: A Wake-Up Call for Companies

Data Breaches & Data Leaks

- India's Biggest Data Breach? COVID Information of Over 800 Million People Leaked

Cyber Crimes & Incidents

- Pro-Hamas Hacktivists Targeting Israeli Entities with Wiper Malware

Vulnerabilities & Exploits

- Exploit Released for Critical Cisco IOS XE Flaw, Many Hosts Still Hacked
- Stop What You're Doing and Patch This Critical Confluence Flaw, Warns Atlassian

Trends & Reports

- Browser Extensions Could Capture Passwords and Sensitive Info as Plain Text

Privacy, Legal & Regulatory

- Biden Wants to Move Fast on AI Safeguards and Will Sign an Executive Order to Address His Concerns
- SEC Charges SolarWinds and Its CISO With Fraud and Cybersecurity Failures

Cybersecurity Awareness Month

- The Daily Cyber Headlines are shared during October at TLP: WHITE for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

ServiceNow Data Exposure: A Wake-Up Call for Companies

Summary

- ServiceNow announced that misconfigurations within the platform could result in unintended access to sensitive data.

Analysis & Action

The default ServiceNow configuration for Simple List allows the data in the tables to be accessed remotely by unauthenticated users. These tables include sensitive data, including content from IT tickets, internal classified knowledge bases, employee details, and more.

ServiceNow has taken steps to fix this issue, but it is still important for organizations to review their Access Control Lists (ACLs) and public widgets to ensure that they are configured correctly.

Organizations should also consider using stricter access control measures, such as IP Address Access Control or Adaptive Authentication.

The article from ServiceNow is available here for review.

Data Breaches & Data Leaks

India's Biggest Data Breach? COVID Information of Over 800 Million People Leaked

Summary

- Indian citizens fall victim to yet another large-scale data incident.

Analysis & Action

More than 800 million Indian citizens had their data compromised. This data includes Aadhaar (unique citizen identification number) and passport details.

The data is made available for purchase on the dark web. A US-based cybersecurity firm discovered the leak after seeing personally identifiable information (PII) records of Indian citizens being sold online. The information's believed source is the Indian Council

of Medical Research (ICMR), which was gathering information during COVID-19, but this has not yet been confirmed.

Indian residents have recently been subjected to a series of data leaks, with threat actors targeting governmental institutions, and this could be the biggest breach yet. This massive data breach highlights the vital need for improved data security measures, as well as the challenges associated with personal data protection in the digital world.

Cyber Crimes & Incidents

Pro-Hamas Hacktivists Targeting Israeli Entities With Wiper Malware

Summary

- A pro-Hamas hacktivist group has been observed using a new Linux-based wiper malware dubbed BiBi-Linux Wiper, targeting Israeli entities.

Analysis & Action

The malware allows attackers to specify target folders and can potentially destroy an entire operating system if it is run with root permissions. The malware can also use multithreading to corrupt files concurrently to enhance its speed and reach, overwriting files, renaming them with an extension, and excluding certain file types from being corrupted.

Arid Viper is the suspected Hamas-affiliated threat actor, and it is believed that the group is organized into two sub-groups, each focused on cyber espionage activities against Israel and Palestine, respectively.

The threat actors use social engineering and phishing attacks as initial intrusion vectors to deploy malware to spy on their victims. Members are advised to perform social engineering and phishing attack simulations with their staff members to ensure their systems remain internally protected.

Vulnerabilities & Exploits

Exploit Released for Critical Cisco IOS XE Flaw, Many Hosts Still Hacked

Summary

- Public exploit code was just released for a critical Cisco IOS XE vulnerability tracked as CVE-2023-20198.

Analysis & Action

Public exploit code for critical Cisco IOS XE vulnerability tracked as CVE-2023-20198 was just made available online.

The vulnerability affecting the web UI feature of Cisco IOS XE Software had already been exploited in zero-day attacks, and over 50,000 devices were allegedly identified as being compromised. The vulnerability allows threat actors to create accounts with full access leading to a full takeover of the device.

Patches for critical vulnerability are available, however, Cisco warns many devices remain unpatched. Members are advised to immediately patch their Cisco devices; in case they have not already done so.

Stop What You're Doing and Patch This Critical Confluence Flaw, Warns Atlassian

Summary

- Atlassian warns of yet another critical Confluence vulnerability.

Analysis & Action

The new vulnerability tracked as CVE-2023-22518, is classified as an improper authorization vulnerability in the Confluence Data Center and Server.

The flaw affects all versions of Confluence and has a CVSS (Common Vulnerability Scoring System) score of 9.1. The company has not clarified how the exploitation can lead to data compromise, but they have stated there were no exploits observed so far.

Members who use Atlassian products are advised to patch immediately. More information on the patches can be accessed here.

Trends & Reports

Browser Extensions Could Capture Passwords and Sensitive Info As Plain Text

Summary

- Concerning reports describe the possible future of threat actors utilizing browser extensions to steal passwords and other private information.

Analysis & Action

Digital security researchers at the University of Wisconsin-Madison uncovered a concerning trend of browser extensions holding private user information, such as passwords, credit card information, and social security numbers, in the HTML source code.

While browser extensions have security implementations against threat actors, other browser extensions can be used to steal users' login information and private data. Out of the 17,300 available browser extensions that the UW-Madison researchers tested, about 12.5% of the browser extensions had permissions available to exploit private data.

A key catalyst to threat actor operations is the accessibility of login information. With browser extensions proposing the possibility of another major cyberattack through these means, members are recommended to observe the permissions given to any browser extensions and evaluate the strength of the security of each extension before downloading.

Privacy, Legal & Regulatory

Biden Wants to Move Fast on AI Safeguards and Will Sign an Executive Order to Address His Concerns

Summary

- President Biden is believed to be signing an executive order to guide artificial intelligence (AI) development.

Analysis & Action

The new sweeping executive order will introduce new protections for consumers, will require industries to develop new safety and security standards and give federal agencies the authority to oversee new AI developments. The executive order will build on current voluntary commitments taken by technology companies and will be part of a broader strategy to regulate AI.

The Defense Production Act will be used by the executive order to require AI developers to share the results of their safety tests and other miscellaneous information with the federal agencies who oversee enforcing the regulations. The National Institute of Standards and Technology is creating the standards to make sure AI is safe and secure. The Commerce Department is leading the charge in its own mark, asking that all AI-generated content be labeled and watermarked.

Members should continue to track this executive order as it makes its way on and past the President's desk. It is important that, if passed, members who develop AI technology follow designated safety and security standards.

SEC Charges SolarWinds and Its CISO With Fraud and Cybersecurity Failures

Summary

- The Securities and Exchange Commission (SEC) has decided to file charges against SolarWinds and its Chief Information Security Officer (CISO), Timothy G. Brown.

Analysis & Action

The allegations stem from suspected fraud and a violation of internal controls, which resulted in a severe cyber-attack.

The corporation was subjected to a two-year cyber-attack by Russian-linked criminals in an operation dubbed SUNBURST, which resulted in the compromising of the company's

Orion monitoring software. The operation allegedly lasted from the company's initial public offering in 2018 until December 2020. During this time, the company committed fraud by misleading potential investors by overstating the company's cybersecurity standards and neglecting to disclose known dangers, despite being aware of inadequacies in their company's cybersecurity practices. Furthermore, the business allegedly provided an incomplete disclosure concerning the December 2020 SUNBURST attack.

While SolarWinds' CEO claims the company did nothing wrong and will fight the charges, the complaint alleges evidence of multiple instances in which designated departments within the company communicated with Brown their concerns and warnings about the state of cyber security concerning the company's assets, which were ignored by the CISO.

Health-ISAC Cyber Threat Level

On October 19, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to Yellow (Elevated). The Threat Level of Yellow (Elevated) is due to threats from concerns regarding hacktivist activity related to the conflict in the Middle East, an uptick in LinkedIn profile impersonations, MFA Bypass, QR code phishing, and the actively exploited Cisco IOS XE bug.

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 Register
Wion news
Tech Xplore
Atlassian
The Hacker News
Security Week
Bleeping Computer
servicenow
Security Week
The Hacker News

Tags

ServiceNow, SolarWinds, Atlassian, Cisco

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