SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

Daily Cyber Headlines

Daily Cyber Headlines ○ TLP:WHITE Alert ID : b0dd2da7 Oct 04, 2024, 07:53 AM

Leading Story

- Cisco Patches Critical Vulnerability in Data Center Management Product

Data Breaches & Data Leaks

- Radiology Provider Exposed Tens of Thousands of Patient Files

Cyber Crimes & Incidents

- North Korean Hackers Using New VeilShell Backdoor in Stealthy Cyber Attacks
- Fake Browser Updates Spread Updated WarmCookie Malware

Vulnerabilities & Exploits

- PoC Exploit Release For Microsoft Office 0-Day Flaw - CVE-2024-38200
- Linux Servers Under Siege: Perfctl Malware Evades Detection For Years

Trends & Reports

- Cloudflare Blocks Largest Recorded DDoS Attack Peaking at 3.8Tbps

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 – October 10, 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

Cisco Patches Critical Vulnerability in Data Center Management Product

Summary

- Patches have been released for a critical vulnerability affecting a Cisco Data Center Management Product.

Analysis & Action

Cisco released patches for multiple vulnerabilities affecting its products, including a critical severity security flaw in its Nexus Dashboard Fabric Controller (NDFC).

The vulnerability, tracked as CVE-2024-20432, affects NDFC's REST API and web UI and could allow an authenticated, remote attacker to execute arbitrary commands on an affected device with network admin privileges. The security flaw stems from improper user authorization and insufficient validation of command arguments.

Successful exploitation of the vulnerability can be achieved when an adversary submits specially crafted commands to an affected REST API endpoint or through the web UI.

Health-ISAC recommends applying the released software updates to affected versions of the NDFC tool to avoid potential exploitation activity.

Data Breaches & Data Leaks

Radiology Provider Exposed Tens of Thousands of Patient Files

Summary

- Threat actors accessed patient data from the I-MED Radiology patient portal due to weak passwords and a lack of multifactor authentication.

Analysis & Action

An unidentified individual has revealed that they illicitly accessed the I-MED Radiology patient portal using stolen login credentials. I-MED Radiology is a top medical imaging provider in Australia that offers various imaging services, such as MRI, CT, X-ray, ultrasound, and nuclear medicine.

The threat actor discovered the credentials in a data breach, indicating the account holder likely used the same login information for multiple services. This method, known as credential stuffing, involves cybercriminals trying leaked credentials on different platforms. By accessing the portal, the threat actor gained unauthorized access to patient information, including full names, dates of birth, gender, scan details, and scan dates. The compromised accounts had weak passwords, lacked two-factor authentication, and were allegedly shared among multiple users.

Health-ISAC recommends implementing strong password policies and multifactor authentication across all organization’s accounts to minimize the risk of a successful credential stuffing attack.

Cyber Crimes & Incidents

North Korean Hackers Using New VeilShell Backdoor in Stealthy Cyber Attacks

Summary

- The North Korean threat group APT37 has been targeting Southeast Asian countries with a new backdoor and remote access trojan (RAT) called VeilShell.

Analysis & Action

The attack chain begins with a phishing email containing a ZIP archive with a Windows shortcut (LNK) file. When the LNK file is launched, it triggers the execution of PowerShell code that decodes and extracts next-stage components. These components include a lure document, a configuration file, and a malicious DLL file. The configuration DLL files are written to the Windows startup folder, and the DLL file is injected into a legitimate executable named dfsvc.exe.

The malware can gather information about files, compress a specific folder into a ZIP archive and upload it back to the C2 server, download files from a specified URL, rename and delete files, and extract ZIP archives.

Researchers noted that the threat actors were patient and methodical, using long sleep times to avoid traditional heuristic detections. Once VeilShell is deployed, it does not execute until the next system reboot. The campaign represents a sophisticated and stealthy operation targeting Southeast Asia leveraging multiple layers of execution, persistence mechanisms, and a versatile PowerShell-based backdoor RAT to achieve long-term control over compromised systems.

Fake Browser Updates Spread Updated WarmCookie Malware

Summary

- A new FakeUpdate campaign is luring people into installing malware by pretending to be browser and application updates.

Analysis & Action

A recently discovered FakeUpdate campaign in France uses compromised websites to display fake browser and application updates, spreading a new version of the WarmCookie backdoor.

This attack is orchestrated by a threat group named SocGolish. It tricks users with fake update prompts for various applications, such as web browsers, Java, VMware Workstation, WebEx, and Proton VPN. When users click on these fake updates, malicious payloads are downloaded, resulting in an infection.

Health-ISAC recommends raising awareness among staff about different types of social engineering attacks to minimize the risk of an employee downloading an update from an unverified source, potentially resulting in network compromise.

Vulnerabilities & Exploits

PoC Exploit Released For Microsoft Office 0-Day Flaw - CVE-2024-38200

Summary

- A recently disclosed vulnerability relating to Microsoft Office now has proof-of-concept code available, with the potential to allow threat actors to capture users' hashes.

Analysis & Action

Security researchers have recently uncovered and released details on an exploit pertaining to Microsoft Office. The exploit can expose users' NTLMv2 hashes to threat actors.

The vulnerability has been marked as CVE-2024-38200, with potential to impact various versions of Microsoft Office like Office 2016 and 2019, Microsoft 365 Applications for Enterprise, and Office LTSC 2021. The exploit was published onto GitHub and details methods to exploit the flaw with use of Office URI Schemes. Caution should be practiced against enabling automatic logins for user authentication as they will only benefit the exploitation at this time. The vulnerability becomes more dangerous when used in tandem with Group Policy Objects or GPO configurations. Microsoft has since released a patch that fixes some of the issues, but security experts are still sharing recommendations for personal protection.

This highlights the need for consistent patching of devices and implementations of mitigation strategies to help act against these vulnerabilities. Recommendations suggest the restriction of NTLM traffic to remote servers and blocking outbound traffic from suspicious ports. Additionally, the inclusion of users in protected security groups could help work against the threat actors looking to exploit the vulnerability.

Linux Servers Under Siege: Perfctl Malware Evades Detection For Years

Summary

- Alerts of malware by the name of perfctl have been identified as active for the past 3-4 years, causing many exploits.

Analysis & Action

Researchers uncovered malware capable of exploiting over 20,000 server misconfigurations.

The malware uses discrete action, lying dormant when servers are in use to avoid detection from system checks and activating when it notices idle periods using rootkits for masking. The malware exploits multiple vulnerabilities, one impacted vulnerability has been CVE-2021-4043, the Polkit vulnerability. The malware scales its privileges and gains deeper access systems, copying itself into directories and disguising itself as legitimate processes. In the past, there have been a number of reports of odd system behavior linked to malware with high CPU usage and performance issues, which now have the potential to be linked to perfctl malware.

Threat actors commonly use malware attacks to infiltrate users' systems for data and sensitive information, further highlighting the need for security practices. Health-ISAC recommends inspecting untrusted binaries and monitoring resource usage, including capturing network traffic.

Trends & Reports

Cloudflare Blocks Largest Recorded DDoS Attack Peaking at 3.8Tbps

Summary

- A massive DDoS attack targeted the financial services, internet, and telecommunications sectors.

Analysis & Action

A record-breaking distributed denial-of-service (DDoS) attack recently targeted organizations in the financial services, internet, and telecommunications sectors. The month-long campaign, which featured over 100 hyper-volumetric attacks, peaked at an astonishing 3.8 terabits per second (Tbps).

These attacks, which overwhelmed target networks with massive amounts of data, were primarily aimed at the network and transport layers. Many exceeded 2 billion packets per second (pps) and 3 Tbps. The threat actor behind the campaign exploited a network of compromised devices, including numerous Asus home routers, MikroTik systems, DVRs, and web servers. These devices, spread across the globe with significant concentrations in Russia, Vietnam, the U.S., Brazil, and Spain, were used to launch the attacks.

Cloudflare, the internet infrastructure company that mitigated the attacks, reported that the largest spike, peaking at 3.8 Tbps, lasted 65 seconds. The malicious devices primarily utilized the User Datagram Protocol (UDP) on a fixed port, a protocol known for its fast data transfers but lack of formal connection establishment.

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 04, 2024, 11:59 PM

Reference | References

Security Online
Security Week
Bleeping Computer
Bleeping Computer
The Hacker News
Malwarebytes Labs
cybersecuritynews

Tags

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