Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 0019e57d | Oct 10, 2024, 06:41 AM

Today's Headlines:

Leading Story

- Fortinet RCE Flaw Now Exploited in Attacks

Data Breaches & Data Leaks

- Customer Data Compromised In MoneyGram Security Breach
- CreditRiskMonitor Data Breach Impacts Employee Information

Cyber Crimes & Incidents

- Awaken Likho APT Group Targets Russian Government With A New Implant

Vulnerabilities & Exploits

- Palo Alto Networks Warns of Firewall Hijack Bugs With Public Exploit
- Firefox Zero-Day Under Attack: Update Your Browser Immediately

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- Marriott Settles for $52M After Series of Breaches Affecting Millions

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

Fortinet RCE Flaw Now Exploited in Attacks

Summary

- A critical FortiOS remote code execution (RCE) vulnerability, CVE-2024-23113, is being exploited; immediate patching is advised.

Analysis & Action

The flaw (CVE-2024-23113) affects FortiOS, FortiPAM, FortiProxy, and FortiWeb, and allows threat actors to execute arbitrary code or commands remotely by sending a crafted request. The vulnerability has a CVSS score of 9.8, highlighting its criticality.

The flaw was originally disclosed and patched in February 2024. Health-ISAC recommends immediate patching of Fortinet's devices in cases where this has not already been done.

Data Breaches & Data Leaks

Customer Data Compromised In MoneyGram Security Breach

Summary

- Implications of the September MoneyGram cyberattack have left sensitive customer information in jeopardy.

Analysis & Action

The breach's initial detection was found on September 27. It disrupted IT systems, leaving customers unable to access or transfer funds. However, new discoveries have revealed that

between September 20 and 22, a vast amount of financial and personal information was also stolen in the midst of the attack.

The sensitive data included home and email addresses, social security numbers, government IDs and driver's licenses, customer names, phone numbers, and even transaction details. A further investigation shows no ransomware was involved in the attacks. Instead, social engineering tactics were used to gain access through the company's defenses. The threat actor posed as employees, tricking staff into giving them access to the network, resulting in data exfiltration.

Data breaches are a common strategy threat actors use, highlighting the importance of protecting your data. Health-ISAC recommends utilizing dedicated identity protection software to scan for traces of personal and sensitive information.

CreditRiskMonitor Data Breach Impacts Employee Information

Summary

- CreditRiskMonitor, a company specializing in credit and supply chain risk management, has suffered a data breach.

Analysis & Action

According to a filing the firm made with the SEC, unauthorized access was detected on July 19, 2024. A subsequent investigation revealed that the attacker potentially viewed or copied personally identifiable information (PII) belonging to employees and independent contractors.

Despite the threat actor gaining access to personally identifiable information of employees and contractors, CreditRiskMonitor has advised that customer information was not affected, and their operations were significantly impacted.

Details surrounding the matter have yet to be attributed to a ransomware group; however, CreditRiskMonitor was previously listed as a victim by the Cuba ransomware group in late 2022. Health-ISAC recommends implementing protections that follow cyber security best practices to bolster its security posture against threat actor operations.

Cyber Crimes & Incidents

Awaken Likho APT Group Targets Russian Government With A New Implant

Summary

- Threat actor Awaken Likho is targeting Russian industrial entities and government agencies.

Analysis & Action

Reports from cybersecurity firm Kaspersky uncovered information on a new campaign based on investigations into APT group Awaken Likho. Upon investigation, the group, also known as PsuedoGamaredon and Core Werewolf, continued to set targets for enterprises and entities relating to the Russian government.

The newly uncovered campaign went on from June to August as investigative details pointed to the threat actor moving from UltraVNC's platform to MeshCentral to create means of remote access. Additionally, an implant used by the threat actor was detected, sent through phishing emails containing malicious URLs. Signs point to the group beginning to use the new implant in September, as analysis indicates the use of the malware began in August. Awaken Likho utilizes a 7-Zip archive capable of self-extraction. This archive can show a masked decoy document while installing its MeshAgent tool, in which the AutoIT script will execute MicrosoftStores.exe and launch the tool into MeshAgent. The group continues to expand and enhance its operation as it is expected to continue its attacks on targeted infrastructures.

Health-ISAC recommends vigilance regarding suspicious downloads or links, the utilization of trusted antivirus software, and, if possible, secure internet communications to mitigate the risks of similar cyber attacks.

Vulnerabilities & Exploits

Palo Alto Networks Warns of Firewall Hijack Bugs With Public Exploit

Summary

- Palo Alto Networks has disclosed multiple vulnerabilities affecting PAN-OS firewalls.

Analysis & Action

Palo Alto Networks has warned customers to patch security vulnerabilities in its Expedition solution, which allows attackers to hijack PAN-OS firewalls.

The flaws tracked as CVE-2024-9463, CVE-2024-9464, CVE-2024-9465, CVE-2024-9466, and CVE-2024-9467, can be exploited to access sensitive data, such as user credentials, which can help take over firewall admin accounts. Proof-of-concept has been made available demonstrating how to use the CVE-2024-5910 admin reset flaw with the CVE-2024-9464 command injection vulnerability in a chain to execute arbitrary code on vulnerable Expedition servers.

While there is no reported exploitation, Health-ISAC strongly recommends urgently patching vulnerable Palo Alto Networks devices.

Firefox Zero-Day Under Attack: Update Your Browser Immediately

Summary

- Threat actors are exploiting CVE-2024-9680 in Firefox and Firefox Extended Support Release (ESR).

Analysis & Action

A critical security flaw in Firefox and Firefox Extended Support Release (ESR) has been exploited in the wild.

The vulnerability, identified as CVE-2024-9680, is a use-after-free bug in the Animation timeline component. The flaw allows attackers to execute code remotely on the vulnerable device. The patches have been issued in Firefox 131.0.2, Firefox ESR 128.3.1, and Firefox ESR 115.16.1. The vulnerability could be weaponized in a watering hole attack or drive-by download campaign.

Health-ISAC recommends updating your browsers regularly to minimize the risk of exploitation.

Trends & Reports

Nothing to Report.

Privacy, Legal & Regulatory

Marriott Settles for $52M After Series of Breaches Affecting Millions

Summary

- Marriott faces a $52 million fine due to data breaches that affected more than 344 million people between 2014 and 2020.

Analysis & Action

The recent data breach resulted in a $52 million settlement following an investigation launched by 49 state attorneys general and the District of Columbia after threat actors stole sensitive customer information. In another settlement, Marriott and its subsidiary were required to implement strong cybersecurity measures, and the Federal Trade Commission has committed to monitoring their compliance for 20 years.

Marriott suffered three data breaches affecting millions of customer records. The first breach, in 2014, exposed the payment card information of over 40,000 Starwood customers. The second breach, also in 2014, went undetected for four years and compromised 339 million guest account records. The third breach, in 2018, lasted almost two years and affected 1.8 million customers, exposing their personal information.

Health-ISAC recommends that organizations implement appropriate security measures to reduce the risk of data breaches and protect sensitive information.

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 10, 2024, 05:59 PM

Reference | References

Bleeping Computer
Security Week
The Hacker News
Security Affairs
The Register
bitdefender
Palo Alto Networks
Bleeping Computer

Tags

Firefox Zero-Day, Awaken Likho APT Group, Fortinet RCE Flaw, Palo Alto Networks PAN-OS, Data Breaches

---

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