Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 1b0969b2 | Oct 31, 2024, 06:47 AM

Today's Headlines:

Leading Story

- Fortinet Updates Guidance and Indicators of Compromise Following FortiManager Vulnerability Exploitation

Data Breaches & Data Leaks

- Over 47k Impacted in Texas County Breach

Cyber Crimes & Incidents

- Jumpy Pisces Engages in Play Ransomware

Vulnerabilities & Exploits

- Google Fixed a Critical Vulnerability in Chrome Browser

Trends & Reports

- HID State of Healthcare Security Report Details Rising Cyber & Physical Threats
- Updated FakeCall Malware Targets Mobile Devices with Vishing

Privacy, Legal & Regulatory

- Albany ENT & Allergy Services Pays $500K Penalty and Commits to $2.25M Cybersecurity Investment

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – November 26, 2024, 12:00-01:00 PM ET

    - European – November 27, 2024, 03:00-04:00 PM CET
- T-SIG Webinar for SMB Members – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Additional Information

Leading Story

Fortinet Updates Guidance and Indicators of Compromise Following FortiManager Vulnerability Exploitation

Summary

- Fortinet updated its advisory for critical FortiManager flaw CVE-2024-47575 to include new workarounds and identified indicators of compromise (IoCs).

Analysis & Action

Fortinet updated its advisory for critical FortiManager flaw CVE-2024-47575 with new workarounds and identified indicators of compromise (IoCs).

As a reminder, the flaw was initially disclosed on October 23, when Fortinet published an advisory for the critical vulnerability in the FortiManager fgfmd daemon and announced its exploitation. The vulnerability is related to the FortiGate to FortiManager (FGFM) protocol, allowing remote unauthenticated attackers to execute arbitrary code or commands.

Health-ISAC advises members to familiarize themselves with the new workarounds and IoCs and immediately patch the flaw where possible. More information is available in the previously distributed bulletin Fortinet Notifies Customers about an Exploited 0-Day Flaw in FortiManager.

Data Breaches & Data Leaks

Over 47k Impacted in Texas County Breach

Summary

- After a cyberattack in Wichita County in Texas, the information of over 47,000 residents has been compromised.

Analysis & Action

Investigations on the matter concluded in early September, uncovering a variety of data belonging to 47,784 residents.

The breach included social security numbers, names, government IDs, financial account information, medical treatment data, and residents' health insurance details. Notification regarding the breach was delayed due to the lack of complete address information for individuals who had been impacted by the breach. This comes after a recent event where threat actor Medusa ransomware stole almost 1.5 terabytes of data from a rodeo competition organizer. Cybersecurity experts notified mounted patrol services in light of the incident. At this time, it has not been confirmed whether the two scenarios correlate with one another, as county officials have yet to confirm or deny more information on the disclosed breach.

Threat actors often use data breaches and leaks to obtain ransom payments to fund their organizations, highlighting the need for protective measures against these practices. Health-ISAC recommends its members utilize antivirus software and limit access to data to reduce the chances of these breaches taking place.

Cyber Crimes & Incidents

Jumpy Pisces Engages in Play Ransomware

Summary

- Threat actor Jumpy Pisces is believed to be a key actor in the latest ransomware attack, possibly shifting to collaboration with Play ransomware.

Analysis & Action

Jumpy Pisces is known for their work in financial crimes, ransomware attacks, and cyber espionage. The change in the latest attack, however, shows a shift to ransomware infrastructure, attributed to the belief of affiliation with the Play ransomware group.

Expectations are that future attacks by the threat actor will target a wide variety of victims throughout the globe. The group, mainly known for their activity in espionage, is now being warned against for their ransomware attacks. This comes after a client of Unit 42 contacted response services due to security impacts via Play ransomware. In the investigations, however, they gained high confidence that Jumpy Pisces was able to gain access initially using a user's account that had been compromised.

The threat actor spread Silver, an open-source tool, and their customized malware to further hosts using the Server Message Block (SMB) protocol. With these remote tools deployed, they communicated with their C2 server all the way up until November, leading to Play ransomware deployment. At this time, it is uncertain if the threat actor is now an affiliate with Play ransomware but signifies a collaboration with the threat actor, indicating a trend in the future.

Threat actors use phishing as their most common method of compromising user accounts. Health-ISAC recommends that its members implement email security protocols and filter malicious traffic using web gateways.

Vulnerabilities & Exploits

Google Fixed a Critical Vulnerability in Chrome Browser

Summary

- Apple Security and Engineering Architecture recently reported a critical Chrome vulnerability, which Google has now patched.

Analysis & Action

Apple reported the vulnerability, tracked as CVE-2024-10487, on October 23. An out-of-bounds write issue sparked the vulnerability.

The vulnerability lived within Dawn implementation, a cross-platform and open-source version of implementation methods for WebGPU. It is uncertain whether threat actors could expose the vulnerability while active, but it has since been patched. Additionally, Google was notified of another vulnerability, tracked as CVE-2024-10488. This vulnerability resided in WebRTC, a use-after-free issue that was reported on October 18. The company has also addressed this issue in its latest

release of Chrome 130. Details and links pertaining to the bug will be restricted to users until a majority have applied the necessary patches to their systems.

Google Chrome is a high-priority target of threat actors, and new exploitations are consistent due to its high daily user count. Health-ISAC recommends that its members issue the most up-to-date patches to their systems to ensure they are not susceptible to these vulnerabilities.

Trends & Reports

HID State of Healthcare Security Report Details Rising Cyber & Physical Threats

Summary

- HID released its healthcare security report, detailing information from more than 200 IT and security professionals throughout medical facilities.

Analysis & Action

HID provides information on solutions for physical and cyber assessments and works with various healthcare facilities to improve their awareness.

HIDs report detailed information on the well-documented doubling of ransomware attacks taking place within healthcare. Additionally, they recorded that 77% of individuals believed in stronger digital security integrations to combat the drastic increases that have been seen in recent years with cyber attacks. A further analysis suggests an implementation of digital credentials like mobile and biometric authentication methods, with 32% of facilities having implemented the practice. 56% of facilities have also implemented automated systems, providing real-time notifications for any potential malicious threat actors and allowing for quick response times.

These implementations will likely grow as threat actors continue to bolster their practices, but the barriers to these adaptations remain. 74% of respondents attested budget constraints as a reason for the lack of these services in their facilities. With healthcare becoming a high-priority target for cybercriminals, a bolstered approach to security is imminent.

Though the addition of new protective security practices has proven to be costly, inaction has the potential to be far more harmful. Health-ISAC recommends its members consider a multi-layered

approach to security, integrating management practices into security systems.

Updated FakeCall Malware Targets Mobile Devices with Vishing

Summary

- Threat actors are executing vishing attacks targeting mobile devices to deploy malware identified as FakeCall.

Analysis & Action

The malware known as FakeCall is being deployed in vishing attacks launched against mobile devices. Zimperium's zLabs discovered the activity, in which users receive vishing calls from threat actors posing as legitimate companies to trick them into giving up sensitive information, including credit card details and banking credentials.

The FakeCall attack leverages functions unique to mobile devices, such as voice and short message service (SMS) communications. These communication methods deliver the malware, which includes various capabilities to manipulate mobile devices. Attacks are typically initiated after a user downloads a seemingly innocuous Android Packet Kit (APK) file that installs the malware.

Successfully deployed FakeCall malware allows for the interception and manipulation of outgoing and incoming calls via a command-and-control (C2) server to covertly execute nefarious actions. To defend against vishing attacks, organizations should implement employee awareness training programs to keep users informed about social engineering activities used to compromise mobile devices.

Privacy, Legal & Regulatory

Albany ENT & Allergy Services Pays $500K Penalty and Commits to $2.25M Cybersecurity Investment

Summary

- Albany ENT & Allergy Services paid $500,00 in penalties and invested $2.25 million to strengthen its information security practices.

Analysis & Action

After suffering two ransomware attacks, threat actors gained access to the medical records of more than 213,000 New York patients. As a result, Albany ENT & Allergy Services has agreed to pay a hefty financial penalty of $500,000 in tandem with an investment of $2.25 million to increase information security practices. If the medical practice fails to invest the required $2.25 million, they will be required to pay an additional $500,000 in penalties.

The first intrusion was a ransomware attack that was identified on March 27, 2023, after system files were encrypted. Impacted systems and data were restored by the Albany ENT & Allergy Services' IT vendor; however, the cause of the intrusion was not identified before restoration. The second incident was also a ransomware attack that occurred 10 days later, on April 2, 2023. The compromised systems contained records of 213,935 patients, including names, addresses, birth dates, driver's license numbers, Social Security numbers, diagnoses, test results, and treatment information.

Due to insufficient server logs, the initial access vector was not properly identified. Additionally, despite logs being generated, they were not retained for a reasonable period, and there was a lack of security programs to monitor or analyze server traffic. According to investigations regarding the matter, the initial access vector was assessed to likely have been due to exploiting a vulnerable Cisco VPN firewall. Health-ISAC recommends implementing appropriate security controls, a comprehensive incident response plan, and adequate logging of activity within the network to defend against and respond to cyber-attacks.

Health-ISAC Cyber Threat Level

On October 17, 2024, 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:

The Threat Level of Yellow (Elevated) is due to threats from elections-related smishing campaigns, DPRK remote worker activity, potential repercussions of recent activity in the Middle East, commodity malware, and a recent uptick in ransomware events.

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

Reference | References

Red Packet Security
mimecastprotect
Palo Alto Networks
Security Affairs
HIPAA Journal
scworld
sdmmag
mimecastprotect
Infosecurity Magazine

Tags

FakeCall Malware, Rising Cyber & Physical Threats, Jumpy Pisces, Google Flaw, Play ransomware, Fortinet

---

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