Daily Cyber Headlines

Daily Cyber Headlines	TLP:WHITE	Alert Id: b1be5005	2024-10-24 11:54:57

Today’s Headlines:

Leading Story

- Fortinet Warns of Critical Vulnerability in FortiManager Under Active Exploitation

Data Breaches & Data Leaks

- Data Breach Impacts Health Insurance Company
- Millions Affected in Major Health Data Breach Caused By a Missing Password

Cyber Crimes & Incidents

- Ransomware Gangs Use LockBits Fame To Intimidate Victims in Latest Attacks
- Highlighting TA866/Asylum Ambuscade Activity Since 2021

Vulnerabilities & Exploits

- CISA Warns Recent Microsoft SharePoint RCE Flaw Exploited in Attacks

Trends & Reports

- US Energy Sector Vulnerable to Supply Chain Attacks

Privacy, Legal & Regulatory

- UK Government Weighs Review of Computer Misuse Act to Combat Cybercrime

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 – November 14, 2024 at 11:30 AM ET
- Fall Americas Summit, Phoenix, Arizona - December 2-6, 2024

Leading Story

Fortinet Warns of Critical Vulnerability in FortiManager Under Active Exploitation

Summary

- Vulnerable FortiManager devices are being targeted by threat actors; Immediate patching of the CVE-2024-47575 is advised.

Analysis & Action
On October 23, Fortinet published an advisory for the critical vulnerability in the FortiManager fgfmd daemon. The flaw tracked as CVE-2024-47575 is being actively exploited. Its CVSS score of 9.8 highlights its criticality.

The vulnerability is related to the FortiGate to FortiManager (FGFM) protocol, allowing remote unauthenticated attackers to execute arbitrary code or commands. Threat actors are using the flaw to exfiltrate data located on FortiManager, including IPs, credentials, and managed device configurations.

Health-ISAC advises immediate patching of the flaw. More information is available in the previously distributed bulletin Fortinet Notifies Customers about an Exploited 0-Day Flaw in FortiManager.

Data Breaches & Data Leaks

Data Breach Impacts Health Insurance Company

Summary

- Around 3,200 individuals had their personal information compromised in the midst of a data breach involving insurer Johnson and Johnson.

Analysis & Action
The insurance firm is named Johnson and Johnson and has no affiliation or connection with the pharmaceutical, biotechnology, and medical technologies company of the same name. Recent reports detail a now-disclosed data breach that took place in mid-August, impacting the network's security.

A deeper investigation into the data breach by a third party discovered the threat actors might have obtained access to insurance practice files. These practice files were kept in a location of the network that has not been disclosed at this time. Additionally, details on the personal information that has been exfiltrated have not been specified. The company has since made statements claiming no misuse of the compromised data to help ease the minds of their customers. The company has also offered credit monitoring and identity restoration services to those impacted by the breach. At this time, no threat actor has claimed responsibility for the insurance firm's attack.

Health-ISAC recommends its members utilize multi-factor authentication to bolster the security of their accounts. In addition, limiting access to sensitive data with heightened security levels can help prevent future data breaches.

Millions Affected in Major Health Data Breach Caused By a Missing Password

Summary

- An unprotected database left online containing highly sensitive customer information.

Analysis & Action
The discovery came from a misconfigured Kibana instance, an open-source exploration tool that stored large volumes of information about customers of multiple hospitals within the Mexican healthcare sector.

Later analysis pointed to software company eCaresoft, containing two Information Systems for Hospitals based on the cloud used by over 30,000 doctors, 65 hospitals, and 110 outpatient care centers. Among the sensitive data leaked were names, nationalities, blood types, religions, birth dates, genders, phone numbers, emails, ethnicities, personal identification, payment requests, and more. The tool was originally intended to visualize data within logs, which was utilized for querying large data sets and indexing. A lapse of management within the database was likely the cause of the breach, aiding threat actors with future attempts to commit acts of phishing, identity theft, and wire fraud. Fortunately, no payment data or health records were exposed, as the database shows, since it was shut down. Additionally, it is unknown if impacted personnel were notified of the breach at this time.

A lack of protection within a database makes it easy for threat actors to administer data breaches and leaks, highlighting the importance of proper security measures. Health-ISAC recommends its members issue security awareness programs to staff to mitigate the risks of similar data breaches and leaks.

Cyber Crimes & Incidents

Ransomware Gangs Use LockBit’s Fame To Intimidate Victims In Latest Attacks

Summary

- Threat actors have capitalized on the fame of the notorious group Lockbit in their recent attack methods while weaponizing cloud service providers.

Analysis & Action
These attacks come after observations of simple storage service or Amazon S3 transfer acceleration abuse were detected. These attacks exfiltrate their victims' data, allowing it to be uploaded to S3 buckets.

Data exfiltration occurs through ransomware artifacts that embed hard-coded AWS service credentials in the cloud. Over 30 samples containing AWS Access Key and Secret Access Keys have been identified, alluding to an active development targeting both Windows and macOS devices. Initialization begins by encrypting files and enumerating root directories after proper data exfiltration. The threat actor will then change the device's wallpaper to mention Lockbit 2.0 as a scare tactic to make victims pay the ransom. Ransomware encounters have seen a 2.75x increase year-over-year as threat actors continue to find new ways to commit these acts, exposing new vulnerabilities in the process.

Health-ISAC recommends that its members issue the most up-to-date patches to their systems. Additionally, to help mitigate the risks of a potential ransomware attack, avoid untrusted attachments, links, or files from sources unbeknownst to you.

Highlighting TA866/Asylum Ambuscade Activity Since 2021

Summary

- A further analysis into experienced threat actor TA866 and its intrusion operations.

Analysis & Action
The threat actor TA866, also known as Asylum Ambuscade, has been active since 2020. TA866 is known for relying on customized tooling to administer its activities post-compromise.

Further research by Cisco Talos points to the threat actors' association with other threat actors; however, they create relationships to aid one another through the stages of their attacks. In addition, the threat actor has deployed several components with malicious intent, including Screenshotter, WasabiSeed, and AHK Bot. The threat actor has also deployed Cobalt Strike, Resident, CSharp-Streamer-RAT, and Rhadamathys on systems they have compromised.

Custom malware is often used by the group furthermore to initiate their chains of infection for intrusion purposes. The malware gathers data and does reconnaissance, the threat actor then analyzes the data to determine if the target is of high value or not. Targets of the threat actors' campaigns see no form of discrimination, observing cases in the United States, Canada, the Netherlands, the United Kingdom, Italy, Austria, and Germany.

As threat actors continue to improve their methods of intrusion, it is important to remain aware and take proper safety precautions to avoid these high-level attacks. Health-ISAC recommends its members use trusted antivirus solutions and implement network monitoring to mitigate risks related to these threat actors.

Vulnerabilities & Exploits

CISA Warns Recent Microsoft SharePoint RCE Flaw Exploited in Attacks

Summary

- CISA recently added a Microsoft SharePoint Server vulnerability to its known exploited vulnerabilities catalog.

Analysis & Action
The Cybersecurity and Infrastructure Security Agency (CISA) recently added CVE-2024-38094 to its known exploited vulnerabilities (KEV) catalog. The vulnerability, which was recently patched, has a CVSS score of 7.2 and can be exploited over the network with no user interaction required.

According to Microsoft’s advisory, successfully exploiting the vulnerability can lead to an authenticated threat actor with Site Owner permissions executing arbitrary code in the context of the SharePoint server.

The turnaround time for the release of proof-of-concept code was fairly quick. After two days of Microsoft providing updates, the release of proof-of-concept code into the wild was identified. At the time of writing, there have been no observances of attacks exploiting the vulnerability. However, it is imperative that organizations apply the updates as risks of exploitation attacks likely increase after the release of proof-of-concept exploit code.

Trends & Reports

US Energy Sector Vulnerable to Supply Chain Attacks

Summary

- The US energy sector faces increased risks of supply chain attacks due to third-party breaches.

Analysis & Action

According to researchers, the US energy sector faces a heightened risk of supply chain attacks, with 45% of security breaches within the past year stemming from third parties. This observation exceeds the global average of supply chain breaches across all other industries, which stands at 29%.

The study found that 90% of attacks on energy companies breached on more than one occasion involved third parties. Additionally, two-thirds of these breaches were linked to external software and IT providers, while one-fifth involved other energy companies.

Exploiting the MOVEit file transfer software vulnerability executed by the Clop ransomware gang is considered the most common cause of third-party breaches in the energy sector, standing at 39%. It is important that organizations implement third-party management security measures, such as vendor risk assessments, to help defend against threats levied by cybercriminals targeting partners as a springboard to compromise others.

Privacy, Legal & Regulatory

UK Government Weighs Review of Computer Misuse Act to Combat Cybercrime

Summary

- The UK government embarks on a new initiative to combat cybercrime.

Analysis & Action

In the UK government's latest vow to treat cybersecurity as a matter of national security to combat cybercrime, the government has decided to review the 1990 Computer Misuse Act. The law was introduced in 1990 due to growing concerns regarding nefarious computer-related activities.

Since its inception, the law has had several amendments stemming from other legislations and events, including the Police and Justice Act of 2006, the News International phone hacking incident in 2011, and the Serious Crime Act of 2015. In its current form, however, the law risks criminalizing cybersecurity professionals who leverage hacking techniques as part of their roles, including researchers and penetration testers.

Last year, to push for a reform of the Computer Misuse Act, an industry group pushed for a legal amendment to be passed that would allow ethical hackers to use a public interest defense. Nonetheless, the law was not passed. While ethical hacking can be a valuable asset to identifying and addressing security gaps, it is important to adhere to guidelines and legal boundaries while they are in place to minimize risks of legal consequences.

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.

Reference(s): Red Packet Security, Cisco Talos, Health-ISAC Threat Advisory System, The Hacker News, MSSP Alert, Security Week, Infosecurity Magazine, Infosecurity Magazine, Fortinet, Tech Radar
Report Source(s): Health-ISAC

Tags: Microsoft SharePoint RCE Flaw, TA866/Asylum Ambuscade, Critical Infrastructure Security, Fortinet FortiManager, LockBit, UK government, 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