DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 16, 2025

Today's Headlines:

Leading Story

- F5 Says Threat Actors Stole Undisclosed BIG-IP Flaws, Source Code

Data Breaches & Data Leaks

- Almost 26,000 Individuals Affected by Data Breach at Methodist Homes of Alabama & Northwest Florida

Cyber Crimes & Incidents

- BlackSuit Ransomware Actors Breached Corporate Environment, Including 60+ VMware ESXi Hosts
- Threat Actors Leverage Judicial Notifications to Deploy Info-Stealer Malware

Vulnerabilities & Exploits

- Windows Agere Modem Driver 0-Day Vulnerabilities Actively Exploited to Escalate Privileges
- CISA Warns of Rapid7 Velociraptor Vulnerability Exploited in Ransomware Attacks

Trends & Reports

- ACSC Reports Surge in Cyberattacks Targeting Australia's Critical Infrastructure, Focus Shifts to Building Resilience
- Data Loss Rising Despite Companies Spending More on Cybersecurity

Privacy, Legal & Regulatory

- Massachusetts Man Behind PowerSchool Incident Gets Four Years in Prison

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas - October 28, 2025, 12:00-01:00 PM ET
  - European – October 29, 2025, 03:00-04:00 PM CET
- Fall Americas Summit – Carlsbad, California – December 1-5, 2025

Leading Story

F5 Says Threat Actors Stole Undisclosed BIG-IP Flaws, Source Code

Summary

- F5 has confirmed that nation-state actors breached company systems and accessed the BIG-IP platform, successfully exfiltrating customer configuration details along with application source code and vulnerability information.

Analysis & Action

The cybersecurity company F5 confirmed an August cyberattack by nation-state actors who compromised company systems and exfiltrated information related to the BIG-IP environment.

The intrusion was first detected on August 9, when the company discovered threat actors had gained access to its internal system, including the BIG-IP platform. F5 discovered that vulnerability information, source code, and configuration data from certain customers were stolen during the breach. There is currently no evidence that threat actors are exploiting the undisclosed flaws or utilizing the stolen information. The company is still identifying the affected customers and reaching out with guidance, but has assured that no other services were impacted by the breach.

Health-ISAC recommends that its members perform regular vulnerability scans, proactively update all software, and monitor network activity to mitigate intrusions and subsequent data breaches.

Data Breaches & Data Leaks

Almost 26,000 Individuals Affected by Data Breach at Methodist Homes of Alabama & Northwest Florida

Summary

- Nearly 26,000 individuals' personal and health data were exposed in a Methodist Homes breach, prompting investigations and free credit monitoring.

Analysis & Action

Three healthcare providers—Methodist Homes, Rockhill Women's Care, and Sierra Vista Hospital—reported data breaches affecting thousands.

Methodist Homes exposed the sensitive data of nearly 26,000 individuals, including Social Security and medical records. Rockhill Women's Care suffered a ransomware attack, resulting in the leak of 20GB of patient data. Sierra Vista Hospital confirmed unauthorized access to patient information in January 2025. All organizations have taken steps to notify affected individuals and strengthen cybersecurity measures, though some breach details remain undisclosed.

Health-ISAC advises its members to strengthen cybersecurity protocols, conduct regular risk assessments, train staff on data protection, implement multi-factor authentication, and use real-time threat monitoring to prevent and respond to data breaches effectively.

Cyber Crimes & Incidents

BlackSuit Ransomware Actors Breached Corporate Environment, Including 60+ VMware ESXi Hosts

Summary

- Blacksuit Ransomware has been observed breaching a prominent corporate environment, compromising credentials for widespread encryption and data theft.

Analysis & Action

Recent attacks from BlackSuit ransomware, also known as Ignolbe Scorpius, have seen the threat actor breach an unnamed manufacturer's operations, devastating their operations.

Detailed by Palo Alto Networks reports, the attack began with a voice phishing (vishing) scam, posing as the unnamed company's IT help desk. From here, employees would be convinced to input their VPN logins into a fake phishing site, allowing attackers to launch a DCSync attack on domain controllers, siphoning off credentials. Threat actors were then able to laterally move throughout systems, deploying IP scanners to chart networks and SMBExec to exploit flaws, maintaining persistence by installing software such as AnyDesk alongside a custom remote access trojan. To remove traces, BlackSuit then locked down hundreds of virtual machines across 60+ VMware ESXi hosts.

Health-ISAC advises its members to prioritize multi-factor authentication and remain wary of confirmation attempts from foreign entities as mitigations.

Threat Actors Leverage Judicial Notifications to Deploy Info-Stealer Malware

Summary

- Colombian users are being targeted by a well-crafted phishing campaign that impersonates official judicial notifications to ultimately deploy the AsyncRAT malware for advanced information-stealing capabilities.

Analysis & Action

Threat actors are targeting Colombian users via a phishing campaign impersonating official judicial notifications to ultimately deploy the AsyncRAT malware for advanced information-stealing capabilities.

The attack chain begins with a well-crafted email, allegedly from the 17th Municipal Civil Court of the Bogotá Circuit, that informs victims of a filed lawsuit. The message leverages an SVG file that, upon execution, redirects users to a fake Attorney General's Office and Citizens' Consultation Portal webpage. Victims are then prompted to download a seemingly official document, which decodes a Visual Basic Script (VBS) file that executes a PowerShell script to deploy a loader. The AsyncRAT is subsequently deployed within a trusted Windows process, providing threat actors the ability to maintain persistence while evading detection.

Health-ISAC encourages its members to conduct regular training sessions on social engineering, employ email filtering solutions, and deploy endpoint detection and response (EDR) tools as mitigation measures to similar phishing campaigns.

Vulnerabilities & Exploits

Windows Agere Modem Driver 0-Day Vulnerabilities Actively Exploited To Escalate Privileges

Summary

- Two critical zero-day flaws in Windows Agere Modem driver have been disclosed confirming active exploitation in the wild.

Analysis & Action

Two severe zero-day flaws in Windows Agere Modem driver, tracked as CVE-2025-24990 and CVE-2025-24052 (both CVSS score of 7.8), have been disclosed by Microsoft.

Both vulnerabilities impact the itmdm64.sys driver, allowing threat actors with low privileges to gain full administrator access. The first flaw, CVE-2025-24990, comes from an untrusted pointer dereference (CWE-822), which has seen active exploitation in the wild. The second, CVE-2025-24052, stems from a stack-based overflow (CWE-121). Active modem use is not needed for threat actors to exploit the flaws, instating a simple local exploit in order to elevate rights rather than interacting with any hardware. At this time, no indicators of compromise (IoCs) have been detailed in disclosures, though highlighting risks of exploitation to drivers, allowing for malicious code execution to impersonate admins.

Health-ISAC advises its members to consider installing the latest patches to systems, regularly audit systems, and phase out outdated components as mitigations.

CISA Warns of Rapid7 Velociraptor Vulnerability Exploited in Ransomware Attacks

Summary

- CISA issued an alert for an exploited vulnerability in Rapid7's Velociraptor EDR tool that has enabled threat actors to escalate privileges and gain full control of endpoints.

Analysis & Action

The Cybersecurity and Infrastructure Security Agency (CISA) issued an alert on a critical vulnerability in Rapid7's Velociraptor endpoint detection and response (EDR) tool that has already been exploited.

The vulnerability–associated with CVE-2025-6264 and recently added to the Known Exploited Vulnerabilities (KEV) catalog–stems from improper default permissions and has recently been exploited in ransomware campaigns. The flaw enabled threat actors to escalate privileges, execute arbitrary commands, and gain full control of the endpoints in cases where initial access was achieved. Mandiant has identified some incidents in which threat actors also leveraged legitimate Velociraptor artifact-gathering features to deploy malicious payloads that evade detection mechanisms. The company has released version 0.7.1 addressing the issue.

Health-ISAC encourages its members to promptly update the software and employ the least privilege principle to mitigate any related exploits.

Trends & Reports

ACSC Reports Surge in Cyberattacks Targeting Australia's Critical Infrastructure, Focus Shifts to Build Resilience

Summary

- Recent reports from the ACSC highlight the persistent targeting of critical infrastructure in Australia by state-sponsored actors, cybercriminals, and hacktivists.

Analysis & Action

The Australian Cyber Security Centre (ACSC)'s recent reports highlight how critical infrastructure continues to be a prime target for state-sponsored actors, cybercriminals, and hacktivists.

Reports attest to this persistence in the amount of critical infrastructure held within organizations, known for supporting Australian national resilience, sovereignty, and prosperity. Critical infrastructure continues to top incident types in the country, accounting for 55% of incidents involving compromised assets, networks, or infrastructures, while 23% are related to DDoS attacks, and 19% involve either compromised credentials or accounts. In response, ACSC has advised Australian businesses to leverage an assumed compromise mindset, marking their assets as key priorities within their organization and giving them the most protection.

Health-ISAC advises its members to reduce reliance on legacy devices and adopt robust logging practices to enhance threat detection and network security..

Data Loss Rising Despite Companies Spending More on Cybersecurity

Summary

- Recent studies highlight that while organizations continue to heavily invest in data protection, data losses continue to rise due to insider-related security incidents.

Analysis & Action

A 2025 Data Security Report from Fortinet has found that despite higher investments into data protection, organizations are seeing an increase in insider-related security incidents.

The report highlights how 72% of organizations raised their budgets for insider risks and data protection within the last year, 77% of which still reported at least one insider-related incident in the past 18 months. 41% of surveyed companies stated the incidents had cost them between $1 million and $10 million, while 9% of incidents exceeded $10 million. Fortinet attests to the rise in a high number of outdated data loss prevention systems, designed for more traditional environments. The report highlights potential operational and reputational risks for organizations going forward, emphasizing proactive remediation.

Health-ISAC advises its members to consider utilizing role-based access controls (RBAC) and streamlining privileged access as mitigating strategies.

Privacy, Legal & Regulatory

Massachusetts Man Behind PowerSchool Incident Gets Four Years in Prison

Summary

- The man behind the 2024 attacks on a telecommunications company and the software provider PowerSchool has been sentenced to four years in prison.

Analysis & Action

Matthew Lane, the 20-year-old responsible for the December 2024 breach and extortion campaign on PowerSchool, has been sentenced to four years in prison.

The incident involved the use of stolen credentials to gain initial access into the software provider's network, which, in turn, granted Lane access to information of millions of students and employees in the United States and Canada. Some of the compromised data might have included contact details, birth dates, social security numbers, and home addresses. The 20-year-old extorted PowerSchool into paying a ransom, alleging to be part of a notable threat group. The court sentence also addressed a secondary attack on a telecommunications company, in which Lane claimed to be part of the same threat group.

Health-ISAC encourages its members to encrypt all data, establish regular backup schedules, and employ multi-factor authentication to mitigate potential data breaches.

Health-ISAC Cyber Threat Level

On September 18, 2025, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level to **Blue (Guarded)**. The Threat Level of **Blue (Guarded)** is due to threats from:

NPM Worm Impact, QR Code Phishing, Typosquatting Campaigns, Remote IT Worker Fraud, and **Job Posting Scams.**

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)	cybersecuritynews, cybersecuritynews 1, hipaajournal, cybersecuritynews 2, radiojamaicanewsonline, industrialcyber, cybersecuritynews 3, cbc, bleepingcomputer, cyware
Report Source(s)	Health-ISAC

Alert ID 95dc5131

View Alert

Share Feedback

was this helpful? |

Tags Velociraptor, Agere Modem, BlackSuit Ransomware, 0-Day, BlackSuit, ESXI, F5 BIG-IP, InfoStealer, VMware, Rapid7

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

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**