

Daily Cyber Headlines

Daily Cyber Headlines

TLP:WHITE

Alert ID : a6caaad8

Oct 31, 2025, 08:19 AM



Today's Headlines:

Leading Story

- Microsoft Windows Cloud Files Minifilter Privilege Escalation Vulnerability Exploited

Data Breaches & Data Leaks

- Sedgebrook & Heartland Health Center Hit with Ransomware Attacks
- Attacker Claims Massive Identity Attack on PII at HSBC USA

Cyber Crimes & Incidents

- Canada Says Hacktivists Breached Water and Energy Facilities
- Major Telecom Backbone Firm Targeted by Nation-State Actors

Vulnerabilities & Exploits

- WordPress Plugin Vulnerability Exposes 7 Million Sites to XSS Attack

Trends & Reports

- Experts Report Sharp Increase In Automated Botnet Attacks Targeting PHP Servers and IoT Devices

Privacy, Legal & Regulatory

- [AHA Urges White House to Streamline AI Rules in Health Care](#)

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
 - Americas - November 25, 2025, 12:00-01:00 PM ET
 - European – November 26, 2025, 03:00-04:00 PM CET
- [Fall Americas Summit](#) – Carlsbad, California – December 1-5, 2025

Additional Information

Leading Story

[Microsoft Windows Cloud Files Minifilter Privilege Escalation Vulnerability Exploited](#)

Summary

- A critical race condition flaw in Microsoft Windows Cloud Files Minifilter driver allows threat actors to escalate privileges and create arbitrary files.

Analysis & Action

A critical flaw in Microsoft's Windows Cloud Minifilter driver, tracked as [CVE-2025-55680](#) (CVSS score 7.8), has been identified, allowing threat actors to elevate privileges and create arbitrary files on systems.

The vulnerability results from a race condition, where threat actors exploit the time-of-check to time-of-use (TOCTOU) vulnerability, alerting a mapped buffer and replacing it with a random character, causing the driver to follow preset junctions to privileged paths. Successful exploitation enables threat actors to drop a malicious DLL, which is used for side-loading attacks. Microsoft has since released patches for the vulnerability as part of its October 2025 Patch Tuesday updates, recommending that users update immediately, as the flaw has been classified as more likely to be exploited.

Health-ISAC advises its members to consider implementing endpoint detections, restricting user privileges, and hardening directory permissions as mitigating strategies.

Data Breaches & Data Leaks

[Sedgebrook & Heartland Health Center Hit with Ransomware Attacks](#)

Summary

- Sedgebrook and Heartland Health Center have confirmed the exposure of sensitive information resulting from ransomware attacks earlier this year.

Analysis & Action

Two healthcare facilities in the United States reported falling victim to ransomware attacks earlier this year, which exposed sensitive patient data.

Sedgebrook, a retirement and nursing facility in Illinois, discovered unauthorized activity on its network earlier in May. According to forensic reports, threat actors remained in the company's network between May 4 and May 5, leveraging ransomware to encrypt patient files. On August 26, the company confirmed that the compromised data included protected health information, contact details, social security numbers, financial records, and other sensitive information. Similarly, Heartland Health Center in Nebraska confirmed a data breach that exposed sensitive data. The incident was first detected on February 4, with confirmation of the data exposure coming in on June 3.

Health-ISAC encourages its members to encrypt all in-transit and stored data, enforce strict access controls, and deploy Endpoint Detection and Response (EDR) solutions as mitigation measures to ransomware attacks.

[Attacker Claims Massive Identity Attack on PII at HSBC USA](#)

Summary

- A threat actor is claiming to have stolen personally identifiable information from HSBC USA customers, potentially affecting millions.

Analysis & Action

A trove of Personally Identifiable Information (PII) belonging to HSBC USA customers is claimed to have been stolen by a threat actor, potentially impacting millions of customers.

Data allegedly stolen in the breach includes full names, physical addresses, email addresses, Social Security numbers, dates of birth, and mobile, home, and work phone numbers. The breach poses risks of security bypass, identity theft, account takeover, SIM swapping, tax and loan scams, credential stuffing, and other threats.

Health-ISAC advises its members to consider strengthening their identity controls, applying least-privilege policies, and regularly tracking spoofed domains as proactive mitigations.

Cyber Crimes & Incidents

[Canada Says Hacktivists Breached Water and Energy Facilities](#)

Summary

- The Canadian Centre for Cyber Security issued an alert regarding hacktivist activity targeting Industrial Control Systems (ICS) following three recent incidents that impacted critical infrastructure.

Analysis & Action

The Canadian Centre for Cyber Security has issued a warning about hacktivist activity targeting internet-accessible Industrial Control Systems (ICS) devices that control critical infrastructure.

Authorities state hacktivists recently exploited exposed ICS components to modify critical industrial controls. The first attack, targeted at a water treatment plant, involved threat actors tampering with logic controllers and automated systems. Threat actors also manipulated an Automated Tank Gauge (ATG) from a Canadian gas and oil firm, triggering false alarms. The last identified incident involved manipulating temperature and humidity levels in a grain drying silo. The alert included recommendations for organizations to protect ICS devices and their components better.

Health-ISAC encourages its members to conduct a review and risk assessment of ICS devices, enforce strong user authentication protocols, and maintain regular patching schedules as mitigation measures.

[Major Telecom Backbone Firm Targeted by Nation-State Actors](#)

Summary

- Ribbon Communications revealed in its quarterly financial report to the SEC a months-long intrusion into the company's leading network, allegedly orchestrated by a nation-state actor.

Analysis & Action

Ribbon Communications' quarterly financial report, recently submitted to the Securities and Exchange Commission (SEC), reveals a months-long intrusion into its IT network allegedly by a nation-state actor.

The company first discovered the intrusion in September 2025. However, initial reports indicate threat actors might have first gained access in December 2024. While there is currently no evidence that the actors exfiltrated sensitive information from Ribbon's main network, the company has reported that some customer files stored on an external device might have been compromised. Investigations are ongoing, and additional details on the breach are yet to be released.

Health-ISAC recommends its members to encrypt all data, consider network segmentation, and actively review network activity to mitigate potential intrusions.

Vulnerabilities & Exploits

[WordPress Plugin Vulnerability Exposes 7 Million Sites to XSS Attack](#)

Summary

- A severe cross-site scripting flaw found in a WordPress Plugin puts millions of websites worldwide at risk.

Analysis & Action

A critical flaw found in WordPress' LiteSpeed Cache allows threat actors to instate cross-site scripting attacks, impacting 7 million websites worldwide.

The flaw, tracked as CVE-2025-12450 (CVSS score of 6.1) stems from the plugin failing to properly clean user-supplied data before it is displayed on the web page. Threat actors can exploit this flaw by creating crafted design links that trick users into interacting with them. Once a user interacts with the malicious link, arbitrary JavaScript code is executed within their browser. Through these attacks, threat actors can steal sensitive information, session cookies, or perform unauthorized actions. WordPress site administrators are advised to update to version 7.6 or newer immediately to mitigate risks.

Health-ISAC advises its members to consider regulating audits and validating user inputs as proactive mitigation measures.

Trends & Reports

[Experts Report Sharp Increase in Automated Botnet Attacks Targeting PHP Servers and IoT Devices](#)

Summary

- Cybersecurity researchers report a surge in automated attacks targeting PHP servers, IoT devices, and cloud gateways.

Analysis & Action

Cybersecurity researchers have noted a significant increase in automated attacks, which have been observed targeting PHP servers, IoT devices, and cloud gateways.

These attacks were primarily attributed to various botnets, including Mirai, Gafgyt, and Mozi, posing risks of credential stuffing, password spray attacks, or stolen credentials. Campaigns enacting these automated attacks often exploit known CVE vulnerabilities and/or cloud misconfigurations, allowing them to take control of exposed systems. PHP servers were seen to be the most prominently targeted of the bunch, often suffering from outdated plugins or themes, misconfigurations, and/or insecure file storage. The most prominent flaws exploited include CVE-2017-9841, CVE-2021-3129, CVE-2022-47945, CVE-2022-22947, and CVE-2024-3721.

Health-ISAC advises its members to ensure devices are kept up to date and restrict public access to cloud infrastructure as mitigating practices.

Privacy, Legal & Regulatory

[AHA Urges White House to Streamline AI Rules in Health Care](#)

Summary

- The American Hospital Association (AHA) issued a formal letter to the Office of Science and Technology Policy (OSTP) requesting revisions and realignment of existing regulations on the use of artificial intelligence within the healthcare industry.

Analysis & Action

The American Hospital Association (AHA) is requesting that lawmakers realign Artificial Intelligence (AI) regulations for the healthcare sector.

The association issued a letter to the Office of Science and Technology Policy (OSTP) urging them to update existing regulations surrounding the use of AI in the medical field. The AHA argues that current legislation hinders innovation and leads to increased administrative costs. The letter also outlined recommendations to synchronize AI policy

with existing frameworks, such as HIPAA and the Food and Drug Administration's medical device protocols, to eliminate redundancy. Lastly, the association requested a more comprehensive approach to cybersecurity regulations that encompasses all entities within the health sector.

Health-ISAC recommends that its members remain vigilant of emerging legislation on the use of artificial intelligence, particularly as such tools continue to be developed and highly used in the industry.

Health-ISAC Cyber Threat Level

On October 16, 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:

F5 Security Incident, Oracle E-Business Suite (C10p) Campaign, Ongoing ClickFix Campaign, Remote IT Worker Fraud, and RedHat Incident.

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

[bleepingcomputer](#)
[cybersecuritynews](#)
[cybersecuritynews 1](#)
[cyware](#)
[outsourcesaccelerator](#)
[securityweek](#)
[thehackernews](#)
[scworld](#)
[hipaajournal](#)

Tags

Microsoft Windows Cloud Files Minifilter, Nation State Actors, IoT, race condition, Cross-site Scripting, XSS, WordPress, Botnet, Microsoft, Privilege Escalation

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