



Daily Cyber Headlines

[Daily Cyber Headlines](#)☐ TLP:WHITE

Alert ID : 91e3fd48

Oct 13, 2026, 04:55 AM



Today's Headlines:

Leading Story

- Japan Declares First Cyberspace Emergency as AI Turns Ransomware into Carpet Bombing

Data Breaches & Data Leaks

- Hospital Operator Nutex Health Confirms Data Stolen in Cyberattack

Cyber Crimes & Incidents

- Everest and Akira Ransomware Groups Name Two New Victims in Latest Cyber Extortion Activity
- CyberXero Uses Claude Code in Campaign That Stole Over 628,000 Ukrainian Records

Vulnerabilities & Exploits

- Critical SonicWall SMA 1000 Flaw Targeted in 135 Exploitation Attempts After Patch
- Threat Actor Exploit CVSS 10.0 Bricksforge WordPress Flaw Enabling Unauthenticated RCE
- Uncovering Vulnerabilities in Danfoss Refrigeration Controllers

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- Nothing To Report

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
 - Americas – October 27, 2026, 12:00 PM - 1:00 PM ET
 - European – October 28, 2026, 03:00-04:00 PM CET
 - APAC – October 30, 2026, 01:00-02:00 PM AEST

Additional Information

Leading Story

Japan Declares First Cyberspace Emergency as AI Turns Ransomware into Carpet Bombing

Summary

- Japan has issued heightened cybersecurity warnings following a surge in ransomware attacks and data breaches affecting major organizations. Security experts warn that AI-assisted attacks are increasing the scale and speed of cyber threats across multiple industries.

Analysis & Action

Japanese cybersecurity authorities issued urgent security warnings following a surge in cyberattacks affecting businesses, government entities, and hospitals. More than 500 incidents were reported during 2026.

Recent incidents exposed sensitive customer information and highlighted supply chain risks. Security experts warn that AI-assisted reconnaissance, phishing, and vulnerability scanning could accelerate large-scale cyberattacks.

Health-ISAC advises its members to strengthen ransomware defenses, prioritize vulnerability patching, enforce multifactor authentication, monitor suspicious network activity, and assess third-party security risks across critical systems.

Data Breaches & Data Leaks

Hospital Operator Nutex Health Confirms Data Stolen in Cyberattack

Summary

- U.S. hospital operator Nutex Health confirmed unauthorized access and theft of sensitive information, including patient, employee, provider, and financial data. The incident raises concerns about patient privacy, data exposure, and potential extortion.

Analysis & Action

Nutex Health confirmed a cyberattack involving unauthorized access and data theft from its network. The company disclosed the incident in August 2026 and initiated forensic investigations and containment measures.

Stolen information included patient, employee, provider, and confidential financial data. The Gentlemen ransomware group claimed responsibility, and Nutex later reported that it had published the stolen data online.

Health-ISAC advises its members to strengthen data exfiltration monitoring, enforce multifactor authentication, segment clinical networks, review privileged access, and maintain incident response and breach notification procedures.

Cyber Crimes & Incidents

Everest and Akira Ransomware Groups Name Two New Victims in Latest Cyber Extortion Activity

Summary

- Everest and Akira ransomware groups reportedly listed Topcon Healthcare and PIC Group, Inc. as new victims on October 12, 2026. The claims raise potential data exposure concerns, although neither incident has been independently confirmed.

Analysis & Action

Threat intelligence monitoring identified new ransomware data leak site listings involving Topcon Healthcare and PIC Group, Inc., attributed to Everest and Akira, respectively, highlighting ongoing cyber extortion activity.

The listings identify the organizations as ransomware targets, raising concerns about potential data exposure and operational risks. Details regarding affected systems, stolen information, and business disruptions remain unavailable.

Health-ISAC advises its members to monitor ransomware leak sites, strengthen endpoint detection, secure remote access, review suspicious authentication activity, and maintain tested backups and incident response procedures.

CyberXero Uses Claude Code in Campaign That Stole Over 628,000 Ukrainian Records

Summary

- A Russian-speaking threat actor tracked as CyberXero used AI-assisted attack tools to compromise WordPress websites and target Ukrainian critical infrastructure. The campaign reportedly exfiltrated over 628,000 records from four Ukrainian organizations.

Analysis & Action

CyberXero conducted an AI-assisted cyberattack campaign that combined automated exploitation of WordPress websites with targeted intrusions into Ukrainian critical infrastructure, using Claude Code and other offensive tools to speed operations.

The operation scanned 4,708 targets, accessed 429 WordPress administration panels, and deployed 32 web shells within 61 seconds. Claude Code supported reconnaissance, exploitation, and post-compromise activities.

Health-ISAC advises its members to patch vulnerable web applications, secure administrative interfaces, monitor unauthorized account activity, investigate suspicious web shells, and strengthen defenses against automated exploitation.

Vulnerabilities & Exploits

Critical SonicWall SMA 1000 Flaw Targeted in 135 Exploitation Attempts After Patch

Summary

- Security researchers detected 135 exploitation attempts targeting a critical SonicWall SMA 1000 vulnerability shortly after the patch was released. The flaw enables unauthenticated server-side request forgery, potentially allowing unauthorized operations on internal appliance functionality.

Analysis & Action

Security researchers detected 135 exploitation attempts targeting CVE-2026-102255, a critical SonicWall SMA 1000 vulnerability rated CVSS 10.0, shortly after its October 6 security update. Health-ISAC [updated](#) its vulnerability bulletin to include updates on active exploitation.

The pre-authentication server-side request forgery flaw allows remote threat actors to access internal appliance functionality. Researchers observed attempts originating from two IP addresses, although successful compromises remain unconfirmed.

Health-ISAC advises its members to apply SonicWall security hotfixes, restrict appliance exposure, review access logs, investigate suspicious requests, and monitor for potential unauthorized access.

Threat Actor Exploit CVSS 10.0 Bricksforge WordPress Flaw Enabling Unauthenticated RCE

Summary

- A vulnerability in the Bricksforge WordPress plugin is being actively exploited, allowing unauthenticated remote code execution through malicious file uploads. Affected websites face risks of unauthorized access, web shell deployment, and persistent compromise.

Analysis & Action

Active exploitation of CVE-2026-85097 has been observed in Bricksforge WordPress installations running versions up to 3.1.8.9. The vulnerability carries a CVSS score of 10.0 and allows unauthenticated remote code execution. For more information, Health-ISAC [published](#) an advisory for this flaw.

Improper file upload validation lets threat actors upload malicious PHP files, run arbitrary commands, and establish persistent access. Exploitation attempts originated from 63 unique IP addresses, although confirmed compromises remain unquantified.

Health-ISAC advises its members to update Bricksforge to version 3.1.8.10 or later, inspect suspicious file uploads, review website integrity, and monitor for unauthorized modifications or persistent access mechanisms.

Uncovering Vulnerabilities in Danfoss Refrigeration Controllers

Summary

- Researchers found software vulnerabilities in Danfoss refrigeration controllers that could allow unauthorized remote access, command execution, or service disruption.

Analysis & Action

Health sector facilities rely on centralized refrigeration controllers to preserve heat-sensitive medical inventory, including vaccines, blood products, pharmaceuticals, and biological samples. Compromising these embedded web interfaces directly threatens cold-chain compliance and inventory viability.

The identified vulnerabilities—ranging from daily access code calculation to remote command execution—allow malicious actors to manipulate temperature thresholds, trigger denial-of-service states, and disrupt vital facility management systems remotely.

Health-ISAC recommends updating Danfoss AK-SM 800A controllers to firmware version R4.3.1 or later, restricting web management interfaces to isolated internal networks or dedicated VPNs, disabling unnecessary internet exposure, and enforcing continuous network monitoring to detect unauthorized administrative sessions.

Trends & Reports

Nothing to Report.

Privacy, Legal & Regulatory

Nothing to Report.

Health-ISAC Cyber Threat Level

On September 17, 2026, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and decided to maintain it at **Yellow (Elevated)**. The Threat Level of **Yellow (Elevated)** is due to threats from:

ShinyHunters Activity, Job Scams, Increase in Vulnerability Reporting, Third-Party Risk, and DPRK IT Worker Fraud.

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

[cyware](#)
[cyware 1](#)
[techtimes](#)
[ciomonitor](#)
[claroty](#)
[thehackernews](#)
[thehackernews 1](#)
[thehackernews 2](#)
[undercodenews](#)

Tags

CyberXero, Carpet-Bombing Attack, Cyberspace Emergency, Bricksforge, CVE-2026-102255, SMA1000, Claude AI, Everest Ransomware, Akira Ransomware, SonicWall, Japan, Data breach, WordPress

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Content Powered by BLACKWIRE Labs:



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