

Daily Cyber Headlines

Daily Cyber Headlines

TLP:WHITE

Alert ID : 4f549197

Oct 09, 2025, 06:04 AM



Today's Headlines:

Leading Story

- Zimbra Collaboration Suite (ZCS) XSS Zero-Day Vulnerability Actively Exploited in Attacks

Data Breaches & Data Leaks

- Electronics Giant Avnet Confirms Breach, Says Stolen Data Unreadable

Cyber Crimes & Incidents

- BatShadow Group Uses New Go-Based Vampire Bot Malware to Hunt Job Seekers
- Chinese Threat Actors Weaponize Open-Source Nezha Tool in New Attack Wave

Vulnerabilities & Exploits

- Critical AWS ClientVPN for macOS Vulnerability Let Attackers Escalate Privileges

Trends & Reports

- Nearly Three in Four U.S. Health Sector Organizations Report Patient Care Disruption Due to Cyber Attacks

Privacy, Legal & Regulatory

- [Teenagers Arrested in England Over Cyberattack on Nursery Chain Kido](#)

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
- [European Summit](#) – Rome, Italy – October 14-16, 2025
- [Fall Americas Summit](#) – Carlsbad, California – December 1-5, 2025

Additional Information

Leading Story

[Zimbra Collaboration Suite \(ZCS\) XSS Zero-Day Vulnerability Actively Exploited in Attacks](#)

Summary

- CISA has released a critical warning regarding a Cross-Site Scripting (XSS) vulnerability in Synacor's Zimbra Collaboration suite, allowing attackers to run arbitrary JavaScript code in victims' sessions.

Analysis & Action

CISA has issued a critical warning of a zero-day flaw in Synacor's Zimbra Collaboration Suite, tracked as CVE-2025-27915 (CVSS 3.1 score 5.4).

The vulnerability, which is being actively exploited in attacks, exists due to an improper neutralization of input during web page generation. More specifically, it stems from insufficient sanitization of HTML content in Internet Calendar System (ICS) files. Exploitation of the flaw occurs with minimal user interaction, beginning once a user views an email message containing the malicious ICS entries. This allows the embedded JavaScript code to execute automatically through an ontoggle event handler, permitting attackers to run arbitrary JavaScript code and leverage legitimate calendar file functions to deliver malicious payloads.

Health-ISAC advises its members to consider implementing email security controls and filtering, as well as sanitizing server input as mitigations against similar vulnerabilities.

Data Breaches & Data Leaks

Electronics Giant Avnet Confirms Breach, Says Stolen Data Unreadable

Summary

- Avnet has confirmed a recent incident in which threat actors gained access to an external cloud-based database storing sales information for EMEA operations, but noted the compromised data is unreadable.

Analysis & Action

The electronics giant, Avnet, has confirmed a data breach to a single external-hosted database that contained business information for operations in the EMEA region, but reported that the compromised data is unreadable.

Avnet said the unreadable information included historical point-of-sale records, customer contact details, and potential sales agreements. The data can only be read with the help of Avnet's proprietary sales tool, which was not impacted by the attack. An undisclosed threat actor claimed the attack on the company, noting it allegedly stole 1.3 terabytes of data and posted plaintext samples of what the company stated was not sensitive information.

Health-ISAC recommends that its members encrypt all in-transit and stored data, perform regular backups, and enforce strong user authentication measures to mitigate potential attacks on cloud-based databases that may result in a data breach.

Cyber Crimes & Incidents

BatShadow Group Uses New Go-Based Vampire Bot Malware to Hunt Job Seekers

Summary

- A Vietnamese threat group, BatShadow, has been observed leveraging social engineering tactics to deploy the Vampire Bot malware and target job seekers.

Analysis & Action

Aryaka Threat Research Lab disclosed a new campaign by the Vietnamese threat group, BatShadow, that leverages social engineering tactics and the Vampire Bot malware to target job seekers and marketing professionals.

The campaign begins with a well-crafted email message that contains a zip archive with masked LNK files that, when clicked on, prompt the download of a PDF file seemingly for a marketing job opening at Marriott. Simultaneously, the LNK file runs a PowerShell

script that downloads the XtraViewer remote desktop connection software, likely for persistence. Once loaded, the PDF document lures victims into clicking a link redirecting users to a fake job description page. The campaign requires users to use Microsoft Edge browsers to bypass default security mechanisms, prompting victims to copy the document URL into the Edge search bar. The action triggers the automatic download of another zip file that contains the Vampire Bot malware. The executable can steal data, capture screenshots, and maintain communication with an attacker-controlled server to deploy additional payloads.

Health-ISAC encourages its members to avoid interacting with suspicious emails and subsequent attachments, educating all staff on social engineering tactics, and deploying endpoint detection tools as mitigation measures.

[Chinese Threat Actors Weaponize Open-Source Nezha Tool in New Attack Wave](#)

Summary

- Chinese threat actors have been observed leveraging log poisoning techniques and exploiting the legitimate monitoring tool, Nezha, to deploy the Gh0st RAT malware, targeting over 100 victims worldwide.

Analysis & Action

Huntress identified a new campaign by Chinese threat actors in which they leverage the legitimate monitoring tool, Nezha, and log poisoning tactics to deliver the Gh0st RAT malware.

Threat actors gain initial access by exploiting a vulnerable phpMyAdmin panel and then using the Antsword web shell for a PHP web shell drop. The tool helps them identify the web server's privileges and download Nezha for remote control. The next stage of the attack chain involves running PowerShell scripts to create antivirus exclusions and deploy the Gh0st RAT. The campaign has already impacted over 100 victims worldwide.

Health-ISAC recommends that its members proactively patch all system vulnerabilities, deploy endpoint detection and response (EDR) solutions, and enforce strong user authentication protocols to mitigate potential compromises.

Vulnerabilities & Exploits

[Critical AWS ClientVPN for macOS Vulnerability Let Attackers Escalate Privileges](#)

Summary

- A critical AWS Client VPN for macOS flaw allows threat actors to escalate privileges locally, creating risk for administration users.

Analysis & Action

A critical AWS Client VPN for macOS flaw tracked as CVE-2025-11462 (CVSS score 7.8) permits threat actors to gain root privileges after abusing the rotation mechanism of a client's log.

The vulnerability impacts AWS Client VPN for macOS versions 1.3.2 through 5.2.0. Threat actors can exploit the flaw after invoking an internal API endpoint. They could then inject arbitrary content into a symlinked file, and once the file has rotated, the crafted content can execute with root privileges. Afterwards, threat actors can trigger an internal API call, writing a custom cron entry that grants root-level password modification privileges. Currently, the vulnerability has only been identified as impacting macOS users, as Windows and Linux clients remain unaffected. AWS has since addressed the flaw in AWS Client VPN version 5.2.1, advising users to upgrade immediately.

Health-ISAC advises its members to consider auditing log directories and apply the principle of least privilege as additional mitigations to similar vulnerabilities.

Trends & Reports

[Nearly Three in Four U.S. Health Sector Organizations Report Patient Care Disruption Due to Cyber Attacks](#)

Summary

- Recent reports highlight the impact health sector organizations face from ongoing cyber attacks.

Analysis & Action

Recent reports from Proofpoint highlight the impacts of cyber attacks on health sector organizations, causing risks to patient lives and burdening operations.

The report states that 72% of health sector organizations that have undergone ransomware, cloud compromise, supply chain attacks, and/or business email compromise have also disrupted patient care. The development comes as a 69% increase in statistics seen the year prior, as 54% of organizations report increased

complications of procedures, 53% report patients staying in facilities longer, and 29% report increased mortality rates, attributing cyber attacks to be a direct result. As these attacks remain persistent, organizations look to embed AI in either cybersecurity (30%) or cybersecurity and patient care (27%) as remediative tactics. The report highlights a call for leadership, addressing gaps in cyber awareness, negligence, and insider risks to mitigate the continuation of these events further.

Health-ISAC advises its members to consider deploying firewalls, regularly auditing security measures, and securing all connected medical devices as mitigations against these attacks.

Privacy, Legal & Regulatory

[Teenagers Arrested in England Over Cyberattack on Nursery Chain Kido](#)

Summary

- British police have arrested two teenagers allegedly responsible for the recent cyberattack on the nursery chain Kido.

Analysis & Action

Two 17-year-old boys were arrested in England for their alleged involvement in the recent cyberattack on the nursery chain, Kido, that resulted in the data breach of sensitive information from thousands of children and their families.

The threat actors had revealed pictures of approximately 20 children as proof of their attack, but had allegedly stolen names, addresses, and contact details of nearly 8,000 kids and their respective carers. The compromised phone numbers were then used for extortion campaigns, as a means to pressure the nursery chain into paying the ransom. Following public discontent, the threat group stopped the extortion campaign and allegedly deleted all stolen material. The teenagers remain in custody for questioning on suspicion of blackmail and computer misuse.

Health-ISAC encourages its members to encrypt all data and proactively review system logs to mitigate potential attacks and subsequent 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.**

Report Source(s)

Health-ISAC

Reference

[aijourn](#)
[cybersecuritynews](#)
[cybersecuritynews 1](#)
[thehackernews](#)
[therecord](#)
[thehackernews 1](#)
[bleepingcomputer](#)

Tags

AWS ClientVPN, Nezha Tool, BatShadow Group, Health Sector, Zimbra Collaboration Suite, 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