



Daily Cyber Headlines

[Daily Cyber Headlines](#)☐ TLP:WHITE

Alert ID : 636d776f

Oct 06, 2026, 04:43 AM



Today's Headlines:

Leading Story

- OpenAI Executive Jason Kwon to Face Grilling at Parliament About AI Breaching Australians' Private Data

Data Breaches & Data Leaks

- 250,000 Patients Impacted by Separate Healthcare Data Breaches

Cyber Crimes & Incidents

- ClingSTUN Backdoor Turns Unpatched Edge Devices Into Covert Proxy Nodes

Vulnerabilities & Exploits

- Attackers Target Rejetto HFS Flaw That Enables Admin Session Forgery and RCE
- New Dell System Update Flaw Lets Threat Actor Gain Root Privileges

Trends & Reports

- Google Narrows Open-Source Bug Bounty Amid Wave of Invalid Automated Reports

Privacy, Legal & Regulatory

- Suspected ShinyHunters Threat Actor Detained in Jordan, Cooperating With FBI

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

OpenAI Executive Jason Kwon to Face Grilling at Parliament About AI Breaching Australians' Private Data

Summary

- OpenAI executives will face a parliamentary inquiry this week to address how their AI models accessed private Australian data.

Analysis & Action

OpenAI executives face a parliamentary inquiry after their AI models improperly accessed sensitive government health data, including internal Medicare and departmental statistics.

This security lapse exposes vulnerabilities in how automated AI agents interact with sensitive public health platforms, highlighting gaps in rapid incident disclosure protocols.

With the rise of these AI-based threats and misalignment incidents, Health-ISAC recommends enforcing stricter API boundaries, implementing real-time activity monitoring, and mandating rapid-response frameworks to prevent unauthorized automated data retrieval.

Data Breaches & Data Leaks

250,000 Patients Impacted by Separate Healthcare Data Breaches

Summary

- Data security incidents at New Jersey-based Clover Health Investments and Texas-based AngMar Management Services compromised the sensitive PII and

PHI of over 250,000 individuals. Stolen data included Social Security numbers, medical histories, diagnosis details, and health insurance information.

Analysis & Action

Two health sector organizations reported major data security incidents affecting more than 250,000 individuals combined. AngMar Management Services, which provides administrative support and operations management for home health and hospice care providers, detected suspicious activity in mid-July 2026. Meanwhile, Clover Health Investments notified the U.S. Department of Health and Human Services (HHS) after identifying compromised patient records on its network systems.

Compromised data elements across the incidents include patient names, dates of birth, Social Security numbers, medical history, diagnosis details, provider names, health insurance details, prescription information, and dates of service. Additionally, the Interlock ransomware group listed AngMar Management Services on its Tor-based leak site in August 2026, claiming to have exfiltrated over 700 gigabytes of unencrypted corporate and patient data prior to the network disruption.

Health-ISAC advises its members to enforce strict access controls and zero-trust network segmentation to safeguard systems hosting sensitive PII and PHI. Organizations should implement robust data loss prevention policies and endpoint monitoring to detect unauthorized bulk file access or anomalous exfiltration channels. Furthermore, health entities should regularly conduct third-party risk assessments, audit administrative service provider permissions, and maintain immutable off-site backups to ensure operational resilience against extortion and ransomware threats.

Cyber Crimes & Incidents

ClingSTUN Backdoor Turns Unpatched Edge Devices Into Covert Proxy Nodes

Summary

- Fortinet researchers identified ClingSTUN, a Linux backdoor exploiting at least 24 known vulnerabilities in internet-facing Internet of Things (IoT) devices and enterprise appliances. The malware abuses legitimate public Session Traversal Utilities for Network Address Translation (STUN) servers to keep compromised devices reachable as proxy nodes.

Analysis & Action

The campaign evolved across three periods, expanding from CVE-2022-36553 in Hytec Inter routers to Realtek, TP-Link, D-Link, and Ivanti Connect Secure flaws CVE-2023-46805 and CVE-2024-21887. Hardcoded exploits for seven additional vulnerabilities turn each infected device into a scanner, while attacker traffic exits through the victim organization's public Internet Protocol (IP) address.

ClingSTUN kills competing malware and watchdog timers, modifies boot scripts for persistence, and masquerades as the system init process. It sends binding requests over User Datagram Protocol (UDP) to public STUN servers to map external ports, and researchers identified no traditional Command and Control (C2) server.

Health-ISAC advises its members to patch or retire exposed routers and gateways, prioritizing the Ivanti Connect Secure vulnerabilities, and segment IoT devices from clinical networks. Organizations should monitor for unexpected STUN requests, recurring UDP keepalive traffic, and processes running from /tmp, correlating these signals rather than blocking public STUN services outright.

Vulnerabilities & Exploits

Attackers Target Rejetto HFS Flaw That Enables Admin Session Forgery and RCE

Summary

- A critical security vulnerability impacting Rejetto HTTP File Server (HFS) is under active exploitation. Tracked as CVE-2026-61500 with a CVSS score of 9.3, the flaw was patched in July 2026. However, threats escalated in September after a security researcher publicly released a Python-based proof-of-concept (PoC) exploit.

Analysis & Action

The vulnerability is a case of session forgery stemming from the use of a weak pseudo-random generator (PRNG), which can produce predictable keys that an attacker can use to gain unauthorized access and seize control of affected systems.

According to VulnCheck's Patrick Garrity, exploitation attempts were detected on October 1, 2026, a day after Horizon3.ai published additional details of the flaw.

Health-ISAC advises members using this software to update to patched version 3.2.1 to mitigate the risk of exploitation and to continually monitor the software for signs of exploitation.

New Dell System Update Flaw Lets Threat Actor Gain Root Privileges

Summary

- Dell released a security advisory warning of a critical vulnerability in its System Update deployment tool. Local attackers with low-privileged access can exploit improper package validation to execute crafted payloads with elevated root or SYSTEM-level permissions.

Analysis & Action

Dell has issued a security update addressing a critical privilege escalation vulnerability in the Dell System Update (DSU) command-line interface deployment utility. DSU is an automated update deployment tool widely utilized by system administrators to maintain firmware, drivers, and system applications across enterprise Dell server fleets and workstations. The vulnerability allows local threat actors who have gained initial foothold on a system with low-level user privileges to escalate their rights to full root or SYSTEM administrative status. For more information, Health-ISAC [published](#) an advisory for this.

Dell confirmed that the security risk affects legacy DSU versions prior to 2.0.0.0 and advised enterprise administrators to apply security patches immediately to mitigate the risk of local privilege escalation.

Health-ISAC advises its members to inventory all server and endpoint deployments that are running the Dell System Update utility and to immediately upgrade affected installations to DSU version 2.0.0.0 or later. Security operations teams should enforce strict endpoint least-privilege policies to restrict standard users from accessing administrative deployment directories or modifying temporary update folders (*C:\ProgramData\Dell\UpdateService*). Additionally, health sector organizations should configure endpoint detection and response (EDR) agents to monitor the DSU executable process for unexpected child process creation, unauthorized file modifications, or abnormal requests for local administrative privileges.

Trends & Reports

Google Narrows Open-Source Bug Bounty Amid Wave of Invalid Automated Reports

Summary

- Google temporarily paused submissions of product vulnerability reports to its Open Source Software Vulnerability Reward Program. The decision addresses an

overwhelming influx of invalid, automated, and AI-generated security reports that overburden open-source maintainers and program triagers.

Analysis & Action

Established in 2022 to incentivize security research across Google-backed open-source projects, the program faced severe operational strain from a surge in low-quality submissions. The pause specifically affects product vulnerability reports, while supply chain security submissions and previously submitted reports remain unaffected, with Google committing to provide a program update in Q1 2027.

The suspension responds to the proliferation of automated vulnerability scanners and AI-assisted triage tools utilized by bug hunters. These automated systems frequently generate high volumes of false positives, hallucinatory exploit paths, and invalid findings lacking actionable proof-of-concept code, exhausting maintainer bandwidth. The move mirrors broader industry adjustments, such as HackerOne's pause on Internet Bug Bounty and recent payout modifications in Google's Chrome and Android reward programs.

Health-ISAC advises its members to refine internal vulnerability management and disclosure processes to mitigate the impact of automated security reports. Organizations maintaining open-source tools or public bug bounty programs should establish strict submission criteria, such as requiring reproducible proof-of-concept scripts and verified impact context, before initiating manual triage. Additionally, enterprise security teams should leverage automated pre-triage filters to validate vulnerability findings internally before allocating engineering resources to remediation.

Privacy, Legal & Regulatory

Suspected ShinyHunters Threat Actor Detained in Jordan, Cooperating With FBI

Summary

- A suspected member of the ShinyHunters cybercrime group, Saif al-Din Khader, was detained in Jordan and is allegedly cooperating with the Federal Bureau of Investigation (FBI).

Analysis & Action

The arrest comes after the threat collective had earlier taken responsibility for altering the appearance of the FBI's portal and allegedly siphoning 2 to 3 terabytes of employee records via an Oracle PeopleSoft flaw.

On September 1, investigators detained another alleged ShinyHunters affiliate in Amsterdam, though the group later denied his involvement. While federal law enforcement refrained from commenting on Khader's detention, authorities confirmed that a rigorous, ongoing investigation into the breach is underway.

Health-ISAC advises its members to remain vigilant about developments involving ShinyHunters, given its history of aggressively targeting healthcare organizations.

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

[fortinet](#)
[bleepingcomputer](#)
[securityweek](#)
[cyware](#)
[securityweek 1](#)
[theguardian](#)
[fortinet](#)
[cbsnews](#)

Tags

OpenAI, Dell System Update, Rejetto HTTP File Server, ShinyHunters, SectopRAT, Dell, Google, Data breach

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