DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 23, 2025

Today's Headlines:

Leading Story

- TP-Link Warns of Critical Command Injection Flaw in Omada Gateways

Data Breaches & Data Leaks

- Oregon Eye Care Provider and New York Children's Center Announce Data Breaches
- Major Patient Data Exposure at Vidal Health Insurance TPA

Cyber Crimes & Incidents

- Chinese Threat Actors Using ToolShell Vulnerability to Compromise Networks of Government Agencies
- Qilin Ransomware Attack Hits Northern Light Technologies and ATR

Vulnerabilities & Exploits

- Multiple GitLab Security Vulnerabilities Let Attacker Trigger DoS Condition

Trends & Reports

- Half of 2025 Ransomware Strikes Target Key Sectors Worldwide: Manufacturing, Health, and Energy

Privacy, Legal & Regulatory

- China Accuses U.S. of Cyberattack on National Time Center

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

TP-Link Warns of Critical Command Injection Flaw in Omada Gateways

Summary

- TP-Link has disclosed and patched four vulnerabilities affecting several Omada gateway devices, which, if exploited, could lead to a full system compromise.

Analysis & Action

TP-Link released two vulnerability bulletins regarding flaws in several Omada gateway devices. If exploited, these flaws could result in a full system compromise.

The first bulletin addresses two high-severity vulnerabilities, CVE-2025-6542 and CVE-2025-6541, with CVSS scores of 9.3 and 8.6, respectively, enabling threat actors to execute arbitrary operating system (OS) commands. The first flaw can be exploited remotely by unauthenticated users; the second, by users with access to the web management interface. Successful exploitation of these vulnerabilities may lead to full system compromise and data theft. The second bulletin warns of CVE-2025-7850 and CVE-2025-7851, with CVSS scores of 9.3 and 8.7, respectively. The first is a command injection flaw that can be exploited to access the web portal, while the second grants root shell access on the underlying OS. TP-Link has released patches for all four vulnerabilities.

Health-ISAC encourages its members to review the vulnerability bulletins for CVE-2025-6541/6542 and CVE-2025-7850/7851 available on Health-ISAC's Threat Intelligence Platform (HTIP) for additional information and recommendations.

Data Breaches & Data Leaks

Oregon Eye Care Provider and New York Children's Center Announce Data Breaches

Summary

- River City Eye Care and Elmcrest Children's Center have confirmed that threat actors gained access to internal networks and exfiltrated sensitive information.

Analysis & Action

Two healthcare providers in Oregon and New York have confirmed recent cyberattacks that breached sensitive patient information.

Elmcrest Children's Center, a support service provider in Syracuse, New York, confirmed threat actors had infiltrated their internal network between March and July 2025, exfiltrating patient data. Initial findings reveal that names, dates of birth, contact information, and medical histories were compromised. Interlock ransomware has claimed responsibility for the attack. Meanwhile, River City Eye Care detected suspicious network activity in Portland, Oregon, in September 2025. The intrusion resulted in the breach of names, addresses, contact details, driver's license numbers, and social security numbers from specific individuals, all of whom are being contacted by the facility. The Genesis threat group has claimed responsibility for the breach.

Health-ISAC advises that its members encrypt all data, secure backups, consider network segmentation, and actively monitor network activity as mitigation to potential data breaches.

Major Patient Data Exposure at Vidal Health Insurance TPA

Summary

A significant breach of patient information at Vidal Health Insurance TPA Pvt. Ltd. has reportedly exposed sensitive health and personal data. The incident highlights the risk to healthcare service data ecosystems and underscores broader vulnerability in TPA operations.

Analysis & Action

Vidal Health Insurance TPA suffered a cyber incident impacting its systems, exposing patient names, insurance details, and medical information. The breach highlights concerns about data protection practices like encryption, access controls, and segmentation in outsourced healthcare services.

The threat actor who claimed the breach is advertising a database containing 326,865 files, which is around 427GB worth of data. The data is being offered for sale for 3,000 USD.

Health ISAC recommends its members implement stronger encryption, enforce strict access controls, improve network segmentation, enhance monitoring, and regularly assess third-party security to prevent future breaches and protect sensitive healthcare data.

Cyber Crimes & Incidents

Chinese Threat Actors Using ToolShell Vulnerability to Compromise Networks of Government Agencies

Summary

- At least three Chinese threat groups have been observed exploiting critical ToolShell vulnerabilities in Microsoft SharePoint servers as part of a cyberespionage campaign targeting critical infrastructure worldwide.

Analysis & Action

Chinese threat actors have been observed exploiting the critical ToolShell vulnerability in the Microsoft SharePoint servers, CVE-2025-53770, to target government agencies and critical infrastructure.

The vulnerability, disclosed and patched earlier this year, stems from improper deserialization of untrusted data that, once exploited, enables unauthenticated code execution. However, the exploit chain often involves the exploitation of CVE-2025-53771, the deployment of malicious payloads, and DLL side-loading techniques. At least three China-based groups have been observed exploiting the flaws: Budworm, Sheathminer, and Storm-2603. Some of the victims identified so far include South American agencies, African government and technology entities, a U.S. university, and a European finance company.

Health-ISAC recommends that its members patch all vulnerable software, as needed, and employ endpoint detection and response solutions as mitigation measures.

Qilin Ransomware Attack Hits Northern Light Technologies and ATR

Summary

The Qilin ransomware group claims to have breached Northern Light Technologies and ATR, stealing 450GB of data and demanding payment within 72 hours.

Analysis & Action

Qilin targeted two organizations operating in different sectors: mining and tunnelling lighting systems, and real estate title information services. Despite differing business models, both suffered mass data

exfiltration accompanied by public proof samples and the customary extortion deadline.

The threat actor claimed to have obtained large volumes of corporate data–a total of 450GB–from both organizations. Posting sample files serves to pressure victims into negotiation. The rapid 72-hour deadline is consistent with recent double extortion tactics, combining encryption with data leak threats.

Health ISAC recommends that its members secure remote access points with MFA and least privilege, encrypt data, segment networks, audit logs, isolate backups, and activate incident response with forensics and legal notifications if data theft occurs.

Vulnerabilities & Exploits

Multiple GitLab Security Vulnerabilities Let Attackers Trigger DoS Condition

Summary

- Several high-severity vulnerabilities impacting GitLab have been found, resulting in denial-of-service flaws. The flaws allow specially crafted payloads to overwhelm systems, alongside access control and authorization bugs affecting authenticated users.

Analysis & Action

GitLab has observed several Denial of Service (DoS) vulnerabilities. These allow crafted payloads to overwhelm systems, and access control and authorization bugs impact users.

The three main vulnerabilities are tracked as CVE-2025-10497 (CVSS 7.5), CVE-2025-11447 (CVSS 7.5), and CVE-2025-11974 (CVSS 6.5), all resulting in denial of service. The first, CVE-2025-10497, impacts event collection, allowing unauthenticated users to send crafted payloads and resulting in an exhaustion of resources. The second, CVE-2025-11447, sees JSON validation GraphQL requests exploited, permitting threat actors to flood systems with malicious payloads, primarily impacting version 11.0. Finally, the third, CVE-2025-11974, arises when large file uploads to sources without authentication consume excessive resources.

GitLab has since released patch versions 18.5.1, 18.4.3, and 18.3.5 to address the flaws, asking users to upgrade immediately. Health-ISAC advises its members to consider deploying firewalls and regularly monitoring network traffic as additional mitigations.

Trends & Reports

Half of 2025 Ransomware Strikes Target Key Sectors Worldwide: Manufacturing, Health, and Energy

Summary

- New reports highlight that global ransomware attacks have surged, with the United States emerging as a top target.

Analysis & Action

New research from KELA highlights a surge in global attacks targeting critical infrastructure, seeing a 34% increase in 2025 as the US emerges as a top target.

4,701 ransomware events were recorded between January and September 2025, much higher than the 3,219 seen within the same period last year. Almost half of these incidents in the US impacted vital sectors such as manufacturing, health, energy, transportation, and finance. The report further highlights that the US has remained the epicenter of ransomware activity as leading groups such as Qilin, Clop, Akira, Play, and Safepay continue to target vital infrastructures, accounting for about 1,000 incidents and 21% of global attacks within the year, followed by Canada, Germany, the United Kingdom, and Italy.

Health-ISAC advises its members to consider adopting a zero-trust security model, limiting user access, and regularly backing up sensitive data as mitigating practices.

Privacy, Legal & Regulatory

China Accuses U.S. of Cyberattack on National Time Center

Summary

- Chinese authorities blame the US for a significant cyberattack targeting the National Time Service Center.

Analysis & Action

Recent reports from China's Ministry of State Security (MSS) claim to have irrefutable evidence proving that the National Security Agency (NSA) attempted a major cyberattack against the National Time Service Center (NTSC).

China claims the attack was intended to steal state secrets belonging to China and conduct cyber espionage against the NTSC. As part of their claims, China pointed to multiple incidents involving credential abuse and system vulnerabilities from 2022 to 2024, highlighting several high-intensity cyberattacks from the NSA against the NTSC's internal network systems.

Health-ISAC advises its members to leverage reputable antivirus software and employ endpoint protection solutions as proactive mitigation against cyberattacks.

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 (Cl0p) 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

Alert ID 9b7d82bb

View Alert

Share Feedback

was this helpful? |

Tags Omada Gateways, ToolShell, Qilin Ransomware, Qilin, Insurance, GitLab, Command Injection, TP-LINK, Denial of Service, Chinese, Data breach

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/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.

Powered by Cyware