DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 21, 2025

Today's Headlines:

Leading Story

- Over 266,000 F5 BIG-IP Instances Exposed to Remote Attacks

Data Breaches & Data Leaks

- Data Breach Hits Security Company Verisure, Impact Considered Limited

Cyber Crimes & Incidents

- American Airlines Subsidiary Envoy Compromised in Oracle Campaign

Vulnerabilities & Exploits

- PoC Exploit Released for Windows Server Update Services Remote Code Execution Vulnerability

- Vulnerability in Dolby Decoder Can Allow Zero-Click Attacks

Trends & Reports

- AI-Driven Social Engineering To Be a Top Cyber Threat for 2026, ISACA Survey Reveals

Privacy, Legal & Regulatory

- SIM Farm Dismantled in Europe, Seven Arrested
- Tech Industry Unites Behind Bipartisan Effort to Urgently Reauthorize US Cyber Threat Information Sharing Law

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

Over 266,000 F5 BIG-IP Instances Exposed to Remote Attacks

Summary

- More than 266,000 F5 BIG-IP instances were found to be exposed to the vulnerabilities compromised during the recently disclosed F5 data breach.

Analysis & Action

Shadowserver Foundation disclosed that over 266,000 F5 BIG-IP instances were exposed online after threat actors breached the company's network.

F5 disclosed the incident last week, on October 15, confirming that nation-state threat actors maintained long-term, persistent access to internal systems. The unauthorized party exfiltrated portions of BIG-IP source code and information on undisclosed vulnerabilities. In an immediate response, the company released patches on the same day to address the vulnerabilities associated with the stolen data. The Shadowserver team subsequently identified more than 142,000 exposed IP addresses in the United States and others in Europe and Asia. F5 has been releasing private advisories and threat-hunting guides for its customers to mitigate potential exploits.

Health-ISAC encourages its members to review the list of shared indicators of compromise (IoCs) on Health-ISAC's Threat Intelligence Portal (HTIP) and review the Cyber Incident alert published last week on the incident.

Data Breaches & Data Leaks

Data Breach Hits Security Company Verisure, Impact Considered Limited

Summary

- The Swedish security company, Verisure, has disclosed a recent data breach to an externally-hosted billing system that may have compromised sensitive information from approximately 35,000 Alert Alarm customers.

Analysis & Action

Verisure has reported a data breach to an external billing partner's system that serves Alert Alarm customers, granting threat actors access to sensitive information from Swedish residents.

The company has confirmed that no internal networks or operations in Latin America and broader Europe have been compromised. Alert Alarm is hosted externally and has no access to the leading network. However, threat actors gained access to the names, contact details, and social security numbers of approximately 35,000 current and former Swedish customers. The company is working with local authorities to investigate the incident further.

Health-ISAC recommends that its members consider network segmentation, employ the principle of least privilege for all applications, and actively monitor network activity to mitigate potential data breaches.

Cyber Crimes & Incidents

American Airlines Subsidiary Envoy Compromised in Oracle Campaign

Summary

- Envoy Air has reported being a victim of a malicious campaign that exploited vulnerabilities in Oracle E-Business Suite.

Analysis & Action

American Airlines subsidiary Envoy Air has claimed it was a victim of a malicious campaign exploiting flaws in Oracle's E-Business Suite (EBS).

The breach comes alongside a recent wave of cyberattacks targeting aviation. Envoy is just one of the more than 60 organizations impacted by the campaign exploiting EBS flaws, which was attributed to Clop ransomware after the threat group claimed responsibility last week. Investigations revealed that only a limited amount of business details were exposed during the attack. Nonetheless, the exposure of internal business data could pose risks of phishing vectors or intelligence leaks.

Health-ISAC advises its members to consider adopting a zero-trust architecture and encrypting sensitive data as mitigating practices.

Vulnerabilities & Exploits

PoC Exploit Released for Windows Server Update Services Remote Code Execution Vulnerability

Summary

- Critical vulnerability in Microsoft Windows Server Update Services allows unauthenticated threat actors to execute remote code, posing risks to enterprise update infrastructures.

Analysis & Action

A critical flaw in Microsoft Windows Server Update, tracked as CVE-2025-59287 (CVSS v3.1 score 9.8), allows unauthenticated threat actors to execute code remotely with SYSTEM privileges.

The flaw stems from unsafe deserialization of untrusted data in Windows Server Update Services AuthorizationCookie handling. The vulnerability exploits this deserialization, targeting the EncryptionHelper.DecryptData() method to decrypt and pass to .NET's BinaryFormatter to be deserialized. Due to a lack of restrictions within the legacy serializer, threat actors can trigger arbitrary code execution through crafted malicious payloads. The vulnerability impacts Windows Server versions from 2012 to 2025. Microsoft has since classified the vulnerability as Exploitation More Likely following a proof-of-concept (PoC) exploit release for the flaw.

Health-ISAC advises its members to consider isolating servers and considering serializers leveraging JSON or XML for stricter validation as mitigations.

Vulnerability in Dolby Decoder Can Allow Zero-Click Attacks

Summary

- A high-severity vulnerability found in Dolby Decoder allows threat actors to exploit for remote code execution.

Analysis & Action

A high-severity flaw in the Dolby Decoder, tracked as CVE-2025-54957 (CVSS score of 7.0), allows threat actors to exploit for remote code execution.

The flaw stems from an out-of-bounds write issue triggered when evolution data is processed. The vulnerability is triggered through malicious audio messages, allowing threat actors to execute remote code without user interaction. Microsoft has since released patches for the flaw as part of its October Patch Tuesday updates, and Google included the patch in its latest ChromeOS update last week.

Health-ISAC advises its members to consider implementing strict input validation and sanitization, disabling unused services, and installing the latest patches as proactive mitigation measures.

Trends & Reports

AI-Driven Social Engineering To Be a Top Cyber Threat for 2026, ISACA Survey Reveals

Summary

- A new ISACA report details AI-driven social engineering to become a leading cyber threat in 2026.

Analysis & Action

A new Tech Trends and Priorities report from ISACA states that AI-driven social engineering attacks will be among the most impactful cyber threats in 2026.

The report details that 63% of IT and cybersecurity professionals consider AI-led social engineering attacks a significant challenge. This comes as AI-driven social engineering begins to surpass known persistent threats, such as ransomware and extortion, which are considered a top threat among 54% of respondents, and supply chain attacks, which are considered a top threat among 35% of respondents. Organizations have been advised to prepare by prioritizing AI governance, modernizing legacy systems, and regularly testing incident response plans to prepare for the continued growth in these attacks.

Health-ISAC advises its members to consider implementing content filtering and regularly conducting security audits as additional mitigation measures.

Privacy, Legal & Regulatory

SIM Farm Dismantled in Europe, Seven Arrested

Summary

- Europol arrested seven individuals in Latvia for their alleged ownership of a sophisticated SIM farm and cybercrime-as-a-service (CaaS) platform that enabled phishing and extortion campaigns worldwide.

Analysis & Action

Under the SIMCartel law enforcement operation, Europol has successfully dismantled a major cybercrime network that leveraged a sophisticated cybercrime-as-a-service (CaaS) platform.

The operation resulted in the arrest of five Latvian nationals and two other suspects operating the CaaS platform from Latvia. The platform allegedly used a SIM farm to provide threat actors worldwide with phone numbers registered to people in over 80 countries. They were then used to create fake social media accounts to hide their identities while simultaneously conducting phishing and extortion campaigns. Europol and investigators from Austria, Estonia, and Latvia, along with Eurojust, seized approximately 40,000 active SIM cards and 1,200 SIM boxes, and dismantled five servers, taking down two websites being used for the group's cybercriminal activity. Initial reports indicate that the CaaS platform enabled the creation of over 49 million online accounts, with financial losses in Austria and Latvia of approximately €5 million.

Health-ISAC advises its members to regularly train all staff on social engineering techniques and employ advanced filtering solutions to block suspicious communications as mitigation measures against similar cybercriminal activity.

Tech Industry Unites Behind Bipartisan Effort to Urgently Reauthorize US Cyber Threat Information Sharing Law

Summary

- Several organizations from the technology sector have shown support for the recently proposed bipartisan legislation, the Protecting America from Cyber Threats Act, which would reauthorize CISA 2015.

Analysis & Action

Several companies in the technology industry have shown support for the bipartisan bill, which is expected to renew the Cybersecurity Information Sharing Act of 2015 (CISA 2015).

The legislation, which was officially named the Protecting America from Cyber Threats Act, was presented earlier this month by Senators Gary Peters and Mike Rounds to re-authorize CISA 2015 and allow companies to continue sharing information relating to cyber threats with the Department of Homeland Security (DHS). Since then, several organizations within the technology industry have shown support, including Palo Alto Networks, SentinelOne, Tenable, Zscaler, the Cybersecurity Coalition, and more. The companies argue that cyber threat information sharing is vital to a collective and proactive stance on cybersecurity and helps safeguard the nation's critical infrastructure.

Health-ISAC encourages its members to actively review and share threat information with their peers for a more informed and resilient health sector.

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

Alert ID d33b2352

View Alert

Share Feedback

was this helpful? |

Tags Dolby Decoder, CISA 2015, Law Enforcement Action, F5 BIG-IP, Artifical Intelligence (AI), Data Breaches, Windows

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/**