DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:GREEN

Nov 04, 2025

Today's Headlines:

Leading Story

- Windows Graphics Vulnerability Allow Remote Attackers to Execute Arbitrary Code

Data Breaches & Data Leaks

- Apache OpenOffice Data Stolen by Akira Ransomware Group

Cyber Crimes & Incidents

- New Phishing Attack Abuses Cloudflare and Zendesk Pages to Steal Logins
- AlphaLocker Ransomware Group Claims Cyber Incident at Riverside Dental Office
- Cybersecurity Workers Charged for Running Ransomware Criminal Operation

Vulnerabilities & Exploits

- Android Security Bulletin Highlights Multiple High Severity Vulnerabilities

Trends & Reports

- AI-Powered Attacks Surge: Organizations Face Major Mobile Security Risks

Privacy, Legal & Regulatory

- FCC to Scale Back Cybersecurity Red Tape on ISPs

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas - November 25, 2025, 12:00-01:00 PM ET
  - European – November 26, 2025, 03:00-04:00 PM CET
- Fall Americas Summit – Carlsbad, California – December 1-5, 2025

Leading Story

Windows Graphics Vulnerabilities Allow Remote Attackers to Execute Arbitrary Code

Summary

- Several vulnerabilities in Microsoft's Graphics Device Interface pose risks to remote threat actors, allowing them to execute arbitrary code or steal sensitive data.

Analysis & Action

Multiple flaws in Microsoft's Graphic Device Interface (GDI) pose risks of threat actors instating remote code execution attacks and/or sensitive information disclosures.

The flaws, tracked as CVE-2025-30388 (CVSS 8.8), CVE-2025-53766 (CVSS 9.8), and CVE-2025-47984 (CVSS 7.5), stem from the improper handling of EMF+ records, which are used in document and image processing for Microsoft Office and web browsers. Threat actors can exploit these flaws by tricking users into opening malicious files, such as altered Word documents or image thumbnails. Successful exploitation of these flaws could result in a complete system compromise without requiring any user interaction. The flaws have been patched in Microsoft's Patch Tuesday update, urging users to apply immediately.

Health-ISAC advises its members to regularly monitor network traffic, disable unnecessary services or ports, and implement the principle of least privilege as additional mitigations.

Data Breaches & Data Leaks

Apache OpenOffice Data Stolen by Akira Ransomware Group

Summary

- Akria Ransomware claims to have exfiltrated 23GB of data from Apache OpenOffice, threatening to leak corporate files soon.

Analysis & Action

Ransomware-as-a-service operation, Akira, has claimed to have stolen 23 gigabytes of data from Apache OpenOffice.

The ransomware group made announcements of the breach on October 29, posting details of the breach to its dark web leak site and threatening to release the information unless a ransom is paid. Though yet to be confirmed by the Apache Software Foundation at the time of reports, the exfiltrated data allegedly includes financial records, confidential files, and employee records containing phone numbers, addresses, social security numbers, and credit card details. If legitimate, the exfiltration could pose risks such as identity theft, targeted phishing campaigns, and financial fraud to those impacted.

Health-ISAC advises its members to regularly maintain data backup and monitor user and system activity as mitigating tactics against data breaches and leaks.

Cyber Crimes & Incidents

Beware of New Phishing Attack That Abuses Cloudflare and Zendesk Pages to Steal Logins

Summary

- A newly found phishing campaign sees threat actors leverage Cloudflare Pages and Zendesk platforms for credential theft on unsuspecting users.

Analysis & Action

A sophisticated phishing campaign has been identified, exploiting trusted platforms Cloudflare and Zendesk to exfiltrate unsuspecting users’ credentials.

The campaign sees threat actors leverage AI-generated phishing pages alongside typosquatting tactics, impersonating customer support portals, and registering domains that closely resemble reputable brands. Threat actors masquerade as operators, requesting users' phone numbers and email addresses, while pretending to provide technical support.

Once threat actors have gained sufficient personal information, victims are instructed to install Rescue, a legitimate remote monitoring tool that becomes dangerous when installed on compromised systems. Once installed, threat actors are granted full remote access to the users’ devices, allowing them to harvest sensitive data and credentials at will.

Health-ISAC advises its members to verify senders before interacting with foreign content, and to avoid foreign links or attachments without verification as a mitigating strategy.

AlphaLocker Ransomware Group Claims Cyber Incident at Riverside Dental Office

Summary

- Riverside Dental Office had a breach after AlphaLocker ransomware operators claimed access to internal systems and posted impacted records, resulting in the exposure of sensitive organizational and operational information.

Analysis & Action

The criminal group publicly listed the dental clinic on its leak portal to demonstrate access and exert pressure on the organization. The compromised data posted by the threat actor included internal files tied to business operations.

The threat actor is known for posting exfiltrated content to strengthen extortion leverage. The listing emphasizes stolen file proof, victim identification, internal directories, and operational documents, which increases the impact of the disclosure.

Health-ISAC advises its members to maintain continuous endpoint visibility, validate privilege boundaries, deploy ransomware-specific behavioral detections, enforce encrypted offline backups, and implement post-compromise containment validation to enhance resilience and response capabilities.

Cybersecurity Workers Charged for Running Ransomware Criminal Operation

Summary

- Cybersecurity professionals faced a breach of trust after prosecutors accused them of participating in a ransomware criminal operation linked to ALPHV BlackCat, which targeted corporate networks across several U.S. states.

Analysis & Action

The indictment stated that these individuals used their cybersecurity positions to support the deployment of ransomware, assist with network encryption, and facilitate illegal extortion activities that impacted multiple business organizations in various U.S. jurisdictions.

The case demonstrates that threat activity can originate from personnel with technical cybersecurity backgrounds, reinforcing the need to verify the use of privileged access within corporate network environments.

Health-ISAC recommends that its members increase privileged user oversight, validate the execution of encryption tools, apply continuous identity controls, enhance internal monitoring, and conduct frequent forensic reviews of incident response and admin-level accounts to reduce insider-driven cyberattack exposure.

Vulnerabilities & Exploits

Android Security Bulletin Highlights Multiple High Severity Vulnerabilities

Summary

- Google had reported multiple security vulnerabilities impacting Android platform components affecting different OEM device models worldwide that may allow elevation of privilege and unauthorized access when exploited by threat actors.

Analysis & Action

Android security bulletin released by Google detailed several high-severity weaknesses identified across the system, framework, kernel, and closed-source vendor modules affecting supported Android versions, requiring urgent patch distribution by OEMs.

Most identified vulnerabilities allowed elevation of privilege and remote code execution vectors at the system level through improper input validation, flawed memory handling, and unprotected permission boundaries, requiring immediate application of vendor-issued updates.

Health-ISAC recommends that its members immediately deploy the latest Android patches across enrolled managed devices, enforce mobile device management controls, and validate that OEM security updates are applied correctly to prevent exploitation attempts on vulnerable Android versions. Continuous mobile fleet vulnerability scanning, prioritizing high-severity elevation vectors, and restricting side loading significantly reduces device compromise exposure.

Trends & Reports

AI-Powered Attacks Surge: Organizations Face Major Mobile Security Risks

Summary

- Recent reports from Verizon highlight a surge in mobile attacks impacting organizations, escalating both risks and vulnerabilities.

Analysis & Action

Findings from Verizon's 2025 Mobile Security Index (MSI) highlight a concerning surge in mobile attacks, posing heightened risks and vulnerabilities to organizations.

The report highlights the challenges organizations face as AI begins to integrate into their workflows, noting that 85% of organizations are experiencing increased threats. The development comes as 93% of organizations report that employees are leveraging generative AI for their tasks, while only 17% have security controls in place to counter AI-assisted attacks. Further highlighted are the heightened risks for smaller organizations, which are more likely to experience significant downtime due to security incidents, often due to budget constraints and limited resources. This emphasizes the importance of these organizations remaining informed and proactive as the landscape continues to evolve.

Health-ISAC advises its members to consider implementing zero-trust controls, segmenting networks, and limiting app permissions as mitigating practices.

Privacy, Legal & Regulatory

FCC to Scale Back Cybersecurity Red Tape on ISPs

Summary

- The FCC is expected to vote on repealing security regulations regarding internet service providers that were previously implemented in the wake of the Salt Typhoon attacks.

Analysis & Action

The Federal Communications Commission (FCC) will vote on repealing security regulations governing internet service providers (ISPs), aimed at establishing a stronger cybersecurity foundation.

The repeal comes as the FCC states that current regulations are an ineffective response to exploitations seen in recent years. The vote is expected to repeal the previous administrative directive issued in response to the threat group Salt Typhoons' activities, which targeted telecommunications companies such as AT&T, Verizon, and Lumen Technologies. Attempts to repeal were initially filed in February of this year by CTIA-The Wireless Association, NCTA – The Internet & Television Association, and USTelecom – The Broadband Association. Leveraging this new approach, the FCC aims to develop a more agile and collaborative cybersecurity framework at both the federal and private levels, with a focus on targeted rulemaking and enforcement.

Health-ISAC advises its members to prioritize system and device hardening, disabling unused services, encrypting sensitive data, and ensuring secure configurations as mitigations.

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.

Reference(s)	cybersecuritynews, scworld, cybersecuritynews 1, reuters, android, sdxcentral, smallbiztrends, redpacketsecurity
Report Source(s)	Health-ISAC

Alert ID dfa58913

View Alert

Share Feedback

was this helpful?  | 

Tags AlphaLocker, Akira, Zendesk, OpenOffice, Cloudflare, Graphics Device Interface (GDI), Artificial Intelligence, Apache, Android, arbitrary code execution, Microsoft

TLP:GREEN TLP:GREEN Limited disclosure, recipients can ONLY share this within their TRUST community. Recipients should consider the information proprietary and may ONLY share TLP:GREEN information with peers and partner organizations within their TRUST community, SHARING IS NOT PERMITTED via social media, public websites and/or other publicly accessible channels.

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/**