



DAILY CYBER HEADLINES

Daily Cyber Headlines



TLP:GREEN

Dec 05, 2025

Today's Headlines:

Leading Story

- CVE-2025-20387: A High-Severity Vulnerability on Splunk

Data Breaches & Data Leaks

- Freedom Mobile Data Breach Exposes Personal Information of Customers
- Nova Ransomware Breach Exposes Brazil's National Primary Health System

Cyber Crimes & Incidents

- Threat Actors Leveraging Foxit PDF Reader to Gain System Control and Steal Sensitive Data
- Microsoft 365 License Verification Error Disrupts Desktop App Access

Vulnerabilities & Exploits

- Critical King Addons Vulnerability Exploited to Breach WordPress Sites

Trends & Reports

- New Report Warns 68% of Actively Serving Phishing Kits Protected by CloudFlare
- 2025 Web Security Overhaul: Five Threats Redefining Cyber Risk

Privacy, Legal & Regulatory

- Virginia Contractors Accused of Wiping Government Databases After Employment Termination

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
 - Americas – December 16, 2025, 12:00-01:00 PM ET
 - European – December 17, 2025, 03:00-04:00 PM CET

Leading Story

[CVE-2025-20387: A High-Severity Vulnerability on Splunk](#)

Summary

- Splunk recently published an advisory about a high-severity vulnerability found in the Splunk Universal Forwarder for Windows, tracked as CVE-2025-20387.

Analysis & Action

This vulnerability, tracked as CVE-2025-20387, is a high-severity vulnerability (with a CVSS Score of 8.0) affecting Splunk Universal Forwarder for Windows, which occurs due to an Incorrect Permission Assignment for a Critical Resource.

This vulnerability occurs during installation or upgrade, assigning overly permissive access rights to the Universal Forwarder installation directory. The vulnerability affects Splunk Universal Forwarder for Windows versions below 10.0.2, 9.4.0 to 9.4.5, 9.3.0 to 9.3.7, and 9.2.0 to 9.2.9.

Health-ISAC advises its members to prioritize patching for affected Splunk versions deployed within their organizations, conduct regular audits and validations, leverage advanced Endpoint Detection and Response (EDR) solutions, monitor SIEM Integrity to flag anomalies immediately, and apply the principle of least privilege. For more information, Health-ISAC published an [advisory](#) for this flaw.

Data Breaches & Data Leaks

[Freedom Mobile Data Breach Exposes Personal Information of Customers](#)

Summary

- Freedom Mobile has disclosed an October data breach that exposed personal information belonging to its customers.

Analysis & Action

Freedom Mobile, a Canadian wireless provider, has disclosed a data breach that occurred on October 23, exposing personal information belonging to its customers.

Investigations into the breach revealed that a threat actor exploited a compromised subcontractor account, gaining access to a limited number of customers' personal information. Information such as first and last names, dates of birth, phone numbers, and mobile account numbers tied to Freedom Mobile. At the time of the reports, the company claimed to have no evidence that the exposed information had been misused. However, it warns customers of potential social engineering attack methods due to the exposure of sensitive information.

Health-ISAC advises its members to regularly assess third-party risk, use encryption for data at rest and in transit, and deploy firewalls as proactive mitigation strategies.

[Nova Ransomware Breach Exposes Brazil's National Primary Health System](#)

Summary

- Brazil's primary health system suffered a significant breach when the ransomware group Nova accessed patient databases and internal systems, potentially compromising millions of medical records.

Analysis & Action

The breach struck Atenção Primária à Saúde, the backbone of Brazil's public primary healthcare services. The intrusion reportedly exposed large volumes of sensitive patient data, undermining trust in the security of Brazil's health data infrastructure.

Attackers from Nova claim they exfiltrated roughly 100 GB of SQL data from systems managed by Fix Tecnologia, which supports the healthcare platform. The leaked data allegedly includes millions of patient records and over fifty million individual entries, covering personal and medical information. This incident highlights the growing trend of ransomware groups targeting healthcare infrastructure, underscoring the critical need for robust data security controls and effective monitoring.

Health-ISAC advises its members to audit all database access logs and enforce strict access controls. Ensure regular encrypted backups of health records are stored separately from production systems. Deploy intrusion detection for abnormal data exfiltration. Promptly reinstall and patch affected systems. Notify the relevant authorities and affected individuals as required for compliance and containment purposes.

Cyber Crimes & Incidents

[Threat Actors Leveraging Foxit PDF Reader to Gain System Control and Steal Sensitive Data](#)

Summary

- Threat actors have been observed targeting job seekers' computers, masking malicious files as legitimate recruiter documents in recent ValleyRAT campaigns.

Analysis & Action

A recently observed campaign, dubbed ValleyRAT, targets active job seekers, exploiting popular Foxit PDF readers to gain remote access to users' systems.

The campaign is primarily spread via email messages containing fake job offers and/or company materials. Upon opening these emails, victims are met with compressed archive files, titled with names designed to seem professional, such as `Overview_of_Work_Expectations.zip`. Upon opening these files, however, victims unknowingly allow remote access trojans to gain access to their system, as threat actors leverage Foxit PDF readers to remove possible user inclination of malicious intent. ValleyRAT, upon installation, grants threat actors complete control over compromised machines, allowing them to monitor user activity and steal sensitive information from browsers.

Health-ISAC advises its members to remain vigilant against unexpected emails with links or attachments and implement network controls, such as email filtering, network segmentation, and firewall protection, as mitigation measures.

[Microsoft 365 License Verification Error Disrupts Desktop App Access](#)

Summary

- Many users found that they could not download desktop apps from Microsoft 365 because a recent service update had broken license verification. This disruption affects access to core office applications across numerous organizations.

Analysis & Action

A recently deployed update in Microsoft 365 introduced a bug that disrupts license verification processes, preventing users from

downloading desktop applications. The issue has been classified as a company-wide incident due to its impact on users trying to install essential productivity tools.

The bug stems from a faulty update to license check components. As a result, even properly licensed users see their downloads blocked. The issue affects all users attempting to download Microsoft 365 desktop apps from the official homepage, regardless of their license status. Microsoft has confirmed that it has developed a fix and is testing it before deploying it broadly.

Health-ISAC advises its members to delay any large-scale Microsoft 365 desktop rollouts until the license check fix is deployed and validated. In the meantime, verify license assignments in the admin portal and consider alternate installation methods. Once the fix is live, run post-deployment validation to ensure downloads succeed and app activations work properly.

Vulnerabilities & Exploits

[Critical King Addons Vulnerability Exploited to Breach WordPress Sites](#)

Summary

- A critical flaw in the King Addons for Elementor plugin has been exploited, allowing threat actors to gain administrative privileges within WordPress sites.

Analysis & Action

A critical flaw within the King Addons for Elementor plugin, tracked as CVE-2025-8489 (CVSS score 9.8), is being exploited by threat actors, allowing them to breach WordPress websites.

The vulnerability, which has been observed being targeted in nearly 50,000 exploit attempts, is described as a privilege escalation flaw. Upon exploitation, the flaw enables unauthenticated threat actors to specify their role without restriction, thereby allowing them to grant themselves administrative roles. WordPress warns that successful exploitation could result in a full site compromise once a threat actor secures administrative privileges, possibly leading to malicious file uploads, content modification, and/or full site takeover. The flaw impacts versions 24.12.92 to 51.1.14; a patch has been made available in King Addons for Elementor version 51.1.35.

Health-ISAC advises its members to consider implementing web application firewalls, limiting administrator access, and maintaining regular backups as additional measures to mitigate risks.

Trends & Reports

[New Report Warns of 68% of Actively Serving Phishing Kits Protected by CloudFlare](#)

Summary

- A new security report issues warnings of online phishing operations primarily leveraging CloudFlare networks.

Analysis & Action

Findings from a new security report have revealed an increase in the use of online phishing operations by threat actors, who are leveraging phishing kits, command-and-control (C2) infrastructure, and malicious payloads.

The report detailed over 42,000 validated URLs and domains associated with these kits, C2 infrastructures, and malicious payloads, suggesting a departure from traditional phishing strategies by a threat actor. Further findings indicate that 17,202 of 25,305 malicious domains tracked (68%) were observed running through CloudFlare's network, with threat actors regularly utilizing CloudFlare's free tier to conceal their hosting servers. As these threats persist, Phishing-as-a-service platforms such as EvilProxy, Tycoon 2FA, and those alike serve as some of the most dangerous developments, operating as adversary-in-the-middle proxies.

Health-ISAC advises its members to consider network segmentation, monitor DNS queries for anomalies, and leverage intrusion prevention systems (IPS) as a mitigating practice.

[2025 Web Security Overhaul: Five Threats Redefining Cyber Risk](#)

Summary

- Major web platforms and services suffered from AI-assisted coding flaws, widespread JavaScript injections, open-source supply-chain compromises, and privacy-tracking mishaps, pushing many organizations to overhaul their web security models.

Analysis & Action

As adversaries harnessed AI, exploited third-party scripts, and weaponized supply-chain vulnerabilities, hundreds of thousands of websites and services became vulnerable, exposing sensitive data,

undermining payment integrity, and revealing the fragility of conventional web defenses.

AI-generated code often worked as expected but contained subtle exploitable flaws that bypassed legacy security tools. A massive campaign successfully injected malicious JavaScript across more than 150,000 websites, compromising payment flows and user sessions. Supply-chain attacks surged: malicious packages slipped into open-source repositories, delivering polymorphic malware that evaded signature-based detection. At the same time, insufficient cookie consent and third-party tracking exposed major privacy and regulatory compliance risks. These events collectively demonstrated that relying on whitelisting or source-based trust is no longer sufficient. Thus, runtime behavior and real-time monitoring have become critical.

Health-ISAC advises its members to inventory and map all third-party dependencies including scripts, libraries, and APIs in live environments; enable continuous runtime behavior monitoring to detect anomalous data flows or unauthorized script actions; treat all AI-generated or auto-imported code as untrusted until subjected to thorough code review, secrets scanning, and penetration testing; enforce continuous privacy-compliance checks to catch consent drift; and shift from periodic audits to real-time monitoring and automated alerting to speed breach detection and containment.

Privacy, Legal & Regulatory

[Virginia Contractors Accused of Wiping Government Databases After Employment Termination](#)

Summary

- Two Virginia brothers have been arrested after allegedly accessing contractor systems and deleting databases following the termination of their employment.

Analysis & Action

The Justice Department has released statements regarding two Virginia brothers who conspired to destroy government databases after termination from their contractor positions.

The brothers, both 34 years old, allegedly gained unauthorized access to contractor systems, issuing commands that prevented others from modifying databases. These databases were later deleted by the brothers, which contained federal investigative documents managed by various agencies and departments. Moreover, the brothers allegedly accessed IRS information and federal tax data for 450 individuals, using a virtual machine for the action. The two now face charges of conspiracy, computer fraud, theft of government records, identity theft, and unauthorized access to a computer.

Health-ISAC advises its members to monitor activity regularly and conduct audits, follow the principle of least privilege, and consider password rotation as a mitigating practice.

Health-ISAC Cyber Threat Level

On November 20, 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:

Glassworm, CEO Impersonation via WhatsApp, Holiday Staffing Shortages, ClickFix Campaigns, and Remote 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.

Reference(s)

[thehackernews](#), [splunk](#), [dailydarkweb](#),
[cybersecuritynews](#), [securityweek](#),
[technadu](#), [cybersecuritynews 1](#),
[cybersecuritynews 2](#), [cyware](#),
[bleepingcomputer](#)



Report Source(s)

Health-ISAC

Alert ID 80bf957b

[View Alert](#)

Share Feedback

was this helpful?  | 

Tags CVE-2025-20387, Nova Ransomware, Foxit PDF, Splunk, Microsoft 365, Cloudflare, Foxit PDF Reader, Phishing Kit, WordPress, 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/>

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

Powered by [Cyware](#)