
Daily Cyber Headlines

Daily Cyber Headlines

TLP:WHITE

Alert ID : f2cb6286

Oct 15, 2025, 08:32 AM



Today's Headlines:

Leading Story

- New PoC Exploit Released for Sudo Chroot Privilege Escalation Vulnerability

Data Breaches & Data Leaks

- 178,000+ Invoices with Customers' Personal Records Exposed from Invoice Platform, Invoicely

Cyber Crimes & Incidents

- Thousands of North Korean IT Workers Using VPNs and Laptop Farms to Bypass Origin Verification
- Massive Botnet Campaign Targeting RDP Services Across the U.S.

Vulnerabilities & Exploits

- SAP Patches Critical Vulnerabilities in NetWeaver, Print Service, SRM

Trends & Reports

- Report: Record Rise in Cyber Attacks on the United Kingdom

Privacy, Legal & Regulatory

- European Commission, ENISA Add GMV to EU Cybersecurity Reserve to Boost Response to Critical Cyber Threats
- Spanish Authorities Dismantle 'GXC Team' Crime-as-a-Service Operation

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
- [European Summit](#) – Rome, Italy – October 14-16, 2025
- [Fall Americas Summit](#) – Carlsbad, California – December 1-5, 2025

Additional Information

Leading Story

[New PoC Exploit Released for Sudo Chroot Privilege Escalation Vulnerability](#)

Summary

- A critical vulnerability in the Sudo utility allows local threat actors to escalate privileges to root level; proof-of-concept has been released as well, raising alarms for Linux administrators.

Analysis & Action

A critical flaw in Sudo utility, tracked as CVE-2025-32463 (CVSS score of 9.3), permits threat actors to escalate privileges to root level with minimal effort.

A proof-of-concept has been released for exploitation of the flaw, as reports indicate active exploitation in the wild, prompting urgent calls for patching. The flaw stems from an improper resolution of paths when the `-chroot` option is in use. For exploitation, threat actors can craft malicious files within controlled directories, making Sudo load arbitrary shared libraries during evaluation, bypassing file restrictions and granting root privileges. Successful exploitation could result in full system compromise, data exfiltration, and/or malware deployment. At the time of reports, Ubuntu and Red Hat have both confirmed the vulnerability to impact their distributions, releasing patches of their own in recent updates.

Health-ISAC advises its members to consider implementing privileged access management (PAM) and conducting regular vulnerability scans as mitigations to similar flaws.

Data Breaches & Data Leaks

[178,000+ Invoices with Customers' Personal Records Exposed from Invoice Platform, Invoicely](#)

Summary

- A publicly accessible database belonging to Invoicely was discovered, exposing 178,159 files containing sensitive personal and financial information of its customers.

Analysis & Action

A publicly accessible database owned by Invoicely was discovered in early October, exposing files in XLSX, CSV, PDF, and image formats of sensitive personal and financial information belonging to Invoicely customers.

The leak resulted from a lack of any encryption within the database, leaving it available to anyone knowing of the URL. Approximately 178,519 files were exposed, including information such as scanned checks, tax filings, and ride-sharing receipts. Due to this exposure, information such as names, addresses, phone numbers, and tax ID numbers was exposed. Furthermore, routing and account details for health sector providers, contractors, and corporate partners were exposed as well. The data leak now presents an amplified risk of possible identity theft and/or spear phishing campaigns from threat actors.

Health-ISAC advises its members to encrypt all sensitive data, ensure regulatory data backups, and regularly conduct security audits and vulnerability assessments as mitigations.

Cyber Crimes & Incidents

[Thousands of North Korean IT Workers Using VPNs and Laptop Farms to Bypass Origin Verification](#)

Summary

- North Korean IT workers continue to be observed infiltrating global technologies, blending in with legitimate workflows and deploying backdoors.

Analysis & Action

The ongoing North Korean IT worker fraud scheme continues to impact global technologies, as actors masquerade themselves as legitimate freelancers to funnel stolen credentials back to their handlers

The scheme has been ongoing since at least 2018, though it gained momentum in mid-2024 following infostealer logs revealing DPRK-owned VPN clients. Malware deployed within the scheme can exfiltrate session tokens, API keys, and SSH configurations, allowing threat actors to maintain access to corporate networks. By 2025, threat actors were observed leveraging platforms such as Slack and GitLab to deploy patches laced with backdoors. A key factor of the scheme is actors' use of laptop farms, rotating IP addresses to emulate user behavior, allowing continual deployment of infostealers while blending in with the genuine activity.

Health-ISAC advises its members to consider bolstering screening processes, verifying physical devices, and regularly monitoring network activity as mitigating strategies.

[Massive Botnet Campaign Targeting RDP Services Across the U.S.](#)

Summary

- Over 300,000 botnet IPs launch coordinated RDP cyberattacks targeting critical U.S. infrastructure, raising major cybersecurity concerns nationwide.

Analysis & Action

Since October 8, 2025, a rapidly expanding botnet—now comprising over 300,000 IP addresses—has launched coordinated attacks on U.S. Remote Desktop Protocol (RDP) infrastructure. Originating from over 100 countries, including Brazil, Argentina, and Singapore, the campaign uses Remote Desktop Web Access timing attacks and RDP login enumeration.

GreyNoise analysis reveals centralized control via similar TCP fingerprints, suggesting a single threat actor. Thus, static defenses are ineffective due to dynamic botnet growth.

Health-ISAC advises its members to implement dynamic IP blocking, disable unused RDP services, enforce multi-factor authentication, monitor for anomalies, update firewalls regularly, and use threat intelligence tools to detect and respond swiftly.

Vulnerabilities & Exploits

[SAP Patches Critical Vulnerabilities in NetWeaver, Print Service, SRM](#)

Summary

- SAP's October 2025 Security Patch Day addressed 16 vulnerabilities, including three critical and two high-severity vulnerabilities, in various SAP products.

Analysis & Action

SAP's October 2025 Security Patch Day addressed 16 new and updated vulnerabilities as part of its monthly releases, including patches for three critical vulnerabilities.

The update adds new protections to the maximum severity deserialization flaw in the NetWeaver AS Java application, CVE-2025-42944, which had been previously addressed in September. A directory transversal flaw in Print Service, tracked as CVE-2025-42937 with a CVSS score of 9.8, was also patched. In addition, SAP released security fixes for an unrestricted file upload vulnerability (CVE-2025-42910) in the Supplier Relationship Management (SRM) system that enables threat actors to potentially upload malicious files. Two high-severity flaws, CVE-2025-5115 and CVE-2025-48913, and 10 medium and low-severity flaws were also identified and patched.

Health-ISAC encourages its members to apply all software patches as promptly as possible and actively scan for system vulnerabilities to mitigate potential exploits.

Trends & Reports

[Report: Record Rise In Cyber-Attacks on United Kingdom](#)

Summary

- An annual review from NCSC indicates a spike in cyber threats impacting the United Kingdom, marking cybersecurity a matter of national resilience.

Analysis & Action

Recent annual reviews from the National Cyber Security Centre (NCSC) allude to an unprecedented rise in cyber threats in the United Kingdom.

Organizations reported a total of 204 nationally significant cyber attacks within the year, more than doubling the 89 seen the year prior. A total of 429 incidents in all were handled, 18 of which were deemed highly significant, meaning they had a serious impact on essential services. The development comes as operations in the health sector, retail, and manufacturing continue to digitize their most critical functions, depending on connected devices and IoT infrastructure. Due to this high level of targeting, the UK's

government has called for board-level focus, marking cybersecurity as a matter of national resilience.

Health-ISAC advises its members to consider enabling firewall protections as initial defenses and deploy endpoint protection solutions as mitigation measures.

Privacy, Legal & Regulatory

[European Commission, ENISA Add GMV to EU Cybersecurity Reserve to Boost Response to Critical Cyber Threats](#)

Summary

- The Spanish multinational, GMV, has been selected by the ENISA and European Commission to join the EU Cybersecurity Reserve.

Analysis & Action

The European Commission and the European Union Agency for Cybersecurity (ENISA) have selected GMV, the Spanish private capital technology business group, to join the EU Cybersecurity Reserve.

Under the EU Cyber Solidarity Act, the EU Cybersecurity Reserve—a small membership of top cybersecurity service providers—aims to promote public-private collaboration, particularly to help prepare entities to manage and respond to cybersecurity incidents. The addition of GMV to the restricted group hopes to strengthen the digital resilience for major critical infrastructure, including the energy, transportation, and healthcare sectors.

Health-ISAC encourages its members to actively share and review information with the membership to mitigate any emerging threats.

[Spanish Authorities Dismantle 'GXC Team' Crime-as-a-Service Operation](#)

Summary

- Spanish authorities, in collaboration with Group-IB, located and arrested a 25-year-old Brazilian national living in northern Spain who allegedly operated a CaaS operation under the GXC Team.

Analysis & Action

Group-IB and Spanish authorities collaborated to arrest a 25-year-old Brazilian, allegedly operating the GCX Team crime-as-a-service (CaaS) operation, in northern

Spain.

The individual, known as GoogleXcoder, allegedly provided Android malware and phishing services to cybercriminals, leveraging phishing kits to target major financial institutions, government entities, and other organizations worldwide. Authorities confirmed the Brazilian operated as a digital nomad, often relocating between multiple homes and thus prompting searches across six different regions in Spain. Several electronic devices were confiscated during the investigation, and the Telegram channel used to communicate with his clients has been deactivated.

Health-ISAC advises that its members conduct regular staff training on social engineering techniques, enforce user authentication measures, and deploy endpoint detection tools to mitigate phishing attacks.

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)

Reference

[industrialcyber](#)
[cybersecuritynews](#)
[cybersecuritynews 1](#)
[cybersecuritynews 2](#)
[securityweek](#)
[securityweek 1](#)
[cyware](#)
[greynoise](#)
[advanced-television](#)

Tags

Invoicely, NetWeaver, ENISA, Sudo, SAP, United Kingdom, United States, RDP, VPN, Linux, Botnet

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