

Daily Cyber Headlines

Daily Cyber Headlines

TLP:WHITE

Alert ID : 3daa520e

Oct 27, 2025, 07:29 AM



Today's Headlines:

Leading Story

- Critical Windows Server WSUS Vulnerability Exploited in the Wild

Data Breaches & Data Leaks

- Albert Heijn Franchisee Targeted by Ransomware Attack, Passports and Personal Information Stolen

Cyber Crimes & Incidents

- Threat Actors Abuse Microsoft 365 Exchange Direct Send to Bypass Content Filters and Harvest Sensitive Data
- North Korean Threat Actors Aim at European Drone Companies

Vulnerabilities & Exploits

- ChatGPT Atlas Stores OAuth Tokens Unencrypted Leads to Unauthorized Access to User Accounts

Trends & Reports

- Counter Ransomware Initiative Stresses Importance of Supply-Chain Security)

Privacy, Legal & Regulatory

- NIS-2 Ushers in New Cybersecurity Obligations to Companies in Germany Through BSIG-E

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

Additional Information

Leading Story

[Critical Windows Server WSUS Vulnerability Exploited in the Wild](#)

Summary

- Microsoft released out-of-band updates for CVE-2025-59287, a critical vulnerability in WSUS, that has already been observed being exploited in the wild.

Analysis & Action

Microsoft released out-of-band (OOB) updates on October 23 to patch a critical vulnerability in the Windows Server Update Service (WSUS) that affects all users with the Server Role feature enabled.

A proof of concept (PoC) for the remote code execution vulnerability CVE-2025-59287 was published by HawkTrace on October 18. Microsoft addressed this vulnerability during this month's Patch Tuesday and included a reference to the PoC in a recent out-of-band (OOB) update. This flaw allows an unauthenticated threat actor to send specially crafted events that trigger unsafe object deserialization, enabling remote code execution. Eye Security and the Dutch National Cyber Security Centre have already detected exploitation of this vulnerability in the wild.

Health-ISAC recommends its members promptly patch the vulnerability and review the latest [Threat Bulletin](#) on the WSUS flaw available on the Health-ISAC Threat Intelligence Platform (HTIP).

Data Breaches & Data Leaks

Albert Heijn Franchisee Targeted by Ransomware Attack, Passports and Personal Information Stolen

Summary

- Albert Heijn's franchisee was recently targeted in a ransomware attack allegedly orchestrated by ThreeAM, which breached sensitive employee data.

Analysis & Action

Albert Heijn's largest franchisee, Bun, was recently the target of a ransomware attack that exposed sensitive employee and owner information.

ThreeAM claimed the attack on October 13, when threat actors published samples of the stolen data, which included names, contact information, identification document numbers, bank account details, and even the passports of the company's owners. The incident impacted over 3,400 current and former employees, making it the second time within the past year that Albert Heijn employee data was exposed after a cyberattack. The company has yet to confirm the group's claims.

Health-ISAC advises its members to encrypt all in-transit and stored data, enforce robust user authentication protocols, and employ endpoint detection and response solutions to mitigate potential ransomware attacks and subsequent data breaches.

Cyber Crimes & Incidents

Threat Actors Abuse Microsoft 365 Exchange Direct Send to Bypass Content Filters and Harvest Sensitive Data

Summary

- Threat actors have been observed leveraging Microsoft 365 Exchange Online's Direct Send Feature to conduct phishing and business email compromise.

Analysis & Action

Microsoft 365's Exchange Online Direct Send feature, intended to allow legacy devices and apps to send emails without needing authentication, has been exploited by threat actors, who have conducted phishing and business email compromise attacks.

Campaigns exploiting the feature often leverage business-themed social engineering lures, such as task approvals, voicemail notifications, and/or payment prompts to trick users into providing credentials or sensitive information. Exploitation has been observed

to circumvent DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting and Conformance (DMARC). Microsoft has since responded to the exploitation issues, introducing a Public Preview of the RejectDirectSend control alongside announcing intentions for future enhancements for new tenants.

Health-ISAC advises its members to remain wary of foreign emails and avoid interaction with links or attachments until verifying the legitimacy of senders as a mitigating strategy.

[North Korean Threat Actors Aim at European Drone Companies](#)

Summary

- Lazarus Group has been targeting European drone manufacturers and other defense sector organizations as part of their large-scale cyberespionage campaign, Operation Dream Job.

Analysis & Action

The North Korean threat group, Lazarus, has been targeting European companies manufacturing drones as part of the large-scale cyberespionage campaign, Operation Dream Job.

According to ESET researchers, the group has been targeting the aerospace, defense, and technology industries for the last five years by providing fake job offers to individuals in the sector. The phony job postings include decoy documents to infect victims' systems with backdoors that, in turn, grant the threat actors access to company data. ESET noted that, since March 2025, Lazarus Group has primarily targeted drone and weapon manufacturers, leveraging the ScoringMathTea remote access trojan (RAT) to gain complete control over targeted systems.

Health-ISAC recommends that its members conduct regular social engineering training for all staff, deploy endpoint detection and response (EDR) tools, and configure firewalls to mitigate similar threats.

Vulnerabilities & Exploits

[ChatGPT Atlas Stores OAuth Tokens Unencrypted Leads to Unauthorized Access to User Accounts](#)

Summary

- A vulnerability in OpenAI's recently released ChatGPT Atlas browser potentially permits unauthorized access to user accounts.

Analysis & Action

OpenAI's newly released ChatGPT Atlas browser has identified a significant vulnerability. The vulnerability bypasses encryption practices and leaves sensitive data exposed to system processes.

The flaw was discovered on October 21 after examining the cache directory following the installation of ChatGPT Atlas. Findings uncovered a SQLite database, which stored functional OAuth tokens with no encryption but were somewhat protected by file permissions, making them readable to all users on Mac devices. The flaw poses a severe security risk, as threat actors could leverage the flaw to deploy malware or other applications to hijack sessions without user awareness. Following observation of the flaw, users have been advised to avoid sensitive tasks on Atlas until the issue is resolved.

Health-ISAC advises its members to monitor their permissions and enable strong access controls, such as multi-factor authentication, as additional mitigation strategies against similar flaws.

Trends & Reports

[Singapore Hosted the Fifth Counter Ransomware Initiative Summit](#)

Summary

- Last week, the Counter Ransomware Initiative's (CRI) fifth annual summit in Singapore discussed the importance of information sharing and released new guidance on supply-chain resilience against ransomware attacks.

Analysis & Action

The International Counter Ransomware Initiative (CRI) hosted its fifth annual summit in Singapore last week and, led by Singapore and the UK, published new guidance on supply-chain security.

During the summit, the CRI, established in 2021 as a global response to international cybercriminal threats, discussed the need for enhanced information sharing between organizations, governments, and the two sectors. In addition, representatives from

Singapore and the United Kingdom released new guidance on the impact of ransomware attacks targeted at supply chain industries. The report calls for a more robust security posture by organizations and governments to mitigate the effects of a ransomware incident on supply chains.

Health-ISAC encourages its members to review and engage with the shared intelligence in the Health-ISAC Threat Intelligence Portal (HTIP) and other communication channels to mitigate emerging threats and build sector-wide resiliency.

Privacy, Legal & Regulatory

[NIS-2 Ushers in New Cybersecurity Obligations to Companies in Germany Through BSIG-E](#)

Summary

- NIS2 is issuing new obligations to expand to a larger set of organizations in Germany as a part of their new BSIG-E documentation.

Analysis & Action

NIS2 is beginning to issue new cybersecurity obligations for a broader scope of organizations throughout Germany as part of their new BSIG-E documentation.

The new cybersecurity law targets companies with at least 250 individuals employed or annual turnovers exceeding 50 million euros in active energy, transport and traffic, finance, health, water, digital infrastructure, and/or aerospace sectors. The law requires these organizations to register with the Federal Office for Information Security, accurately monitor cybersecurity measures taken, introduce measures for documented risk management, and have stricter reporting obligations, among other requirements. Further, within the new obligations, companies that cannot comply with the law will face administrative measures and severe fines.

Health-ISAC advises its members to secure their networks, enabling firewalls and leveraging network intrusion detection systems as proactive mitigations to protect networks and incoming traffic.

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 (C10p) 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

Reference

[cybernews](#)
[cybersecuritynews](#)
[dentons](#)
[cyware](#)
[cybersecuritynews 1](#)
[securityweek](#)
[securityweek 1](#)
[vulcanpost](#)

Tags

WSUS Vulnerability, Counter Ransomware Initiative, ChatGPT, NIS2, Lazarus APT, Microsoft 365, Data Breaches

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