
Weekly Cybersecurity Briefing (28 September – 4 October 2026)

CyberSecBrief Team

CyberSecBrief provides clear, concise cybersecurity briefings that summarise the most relevant developments of the week. The report highlights notable incidents, key themes, and significant activity across the threat landscape, supported by daily updates sourced from trusted feeds and advisories. Its purpose is to offer a practical, time-efficient overview for readers who need a reliable snapshot of current cybersecurity events.

For more briefings, visit [CYBERSECBRIEF.COM](https://cybersecbrief.com).



October 5, 2026

Editorial Analysis

Citrix NetScaler, **Zimbra** and **Cisco SD-WAN vManage** were all being exploited before defenders had public notice of the vulnerabilities. Mandiant places the start of NetScaler exploitation in early September, about three weeks before Citrix published its advisory, while GreyNoise recorded attempts against a NetScaler Gateway three days before the bulletin. Microsoft's timeline puts Zimbra exploitation between the 20 July fix and the 13 August disclosure. Cisco's incident responders discovered the vManage exploitation while investigating a routine support case. The subsequent activity also provided a clearer view of how compromised systems were being used, including WHIPSHOT and SLAPSHOT, which Mandiant found disguised as `.deb` and `.sig` files.

Several of the week's attacks also depended on small differences in how security controls and applications interpret the same request. The **PeopleSoft** attack on the FBI jobs portal used `/%50SEMHub/` to bypass a WAF rule matching `/PSEMHub/`, while **Cisco vManage** had a similar mismatch between its login module and application server over URL decoding. The PeopleSoft victims had added WAF rules without applying Oracle's June patch, leaving the control in place while the vulnerable code remained reachable. In vManage, a single percent-encoded character was enough to bypass authentication.

Enforcement against **ShinyHunters** accelerated during the week without bringing the group's activity to an immediate halt. Dutch police arrested **Pepijn van der Stap** on 15 September, the FBI publicly urged remaining members to surrender, and Reuters reported that **Saif al-Din Khader**, known as Rey, was detained in Jordan and is cooperating with investigators. During the same period, ShinyHunters claimed the FBI jobs breach and escalated its activity to medical records under reportedly more aggressive leadership. Khader's identity and alleged role had been public for more than a year, and Krebs reported last year that he had claimed to have stopped and was cooperating. The group's dark-web site has been offline since Wednesday, but its operators have told Reuters they want no further escalation with the FBI.

Highlights of the Week

Citrix NetScaler Zero-Days Exploited Before Disclosure, Added to CISA Catalogue

Citrix confirmed exploitation of NetScaler ADC and Gateway flaws CVE-2026-88771 and CVE-2026-88772, and CISA added both to its Known Exploited Vulnerabilities Catalogue. Mandiant traced exploitation of CVE-2026-88772 to early September, with WHIPSHOT web shells and SLAPSHOT tunnelling tools disguised as `.deb` and `.sig` files. Sygnia separately found a variant that poisons appliance logs so a maintenance script executes commands as root.

Sources:

- [CISA](#)
- [Citrix](#)
- [Mandiant](#)
- [Sygnia](#)

ShinyHunters Breaches FBI Jobs Portal as Suspected Members Are Detained

ShinyHunters accessed the FBI jobs portal by exploiting Oracle PeopleSoft flaw CVE-2026-35273 through a single-character path substitution that bypassed firewall rules, claiming 2 to 3 terabytes of data. Dutch police arrested Pepijn van der Stap, and the FBI urged remaining members to surrender. Reuters reported suspected member Saif al-Din Khader was detained in Jordan and is cooperating with the FBI.

Sources:

- [Vectra AI](#)
- [Krebs on Security](#)
- [BleepingComputer](#)
- [Reuters](#)

Cisco SD-WAN vManage Authentication Bypass Grants Admin Access

VulnCheck reproduced CVE-2026-76504, a Cisco Catalyst SD-WAN vManage authentication bypass caused by two components disagreeing on how URL-encoded request paths are decoded. A percent-encoded path skips the password check, and one of four hardcoded internal usernames yields an admin session in a single request. Around 1,500 internet-exposed devices were identified, and Cisco disclosed the flaw as an exploited zero-day.

Sources:

- [VulnCheck](#)

Pentagon Breach Exposes Records of About 3 Million Military-Linked Individuals

A breach of the Defense Manpower Data Center exposed unencrypted Social Security numbers and dates of birth for nearly 2.8 million living individuals and 294,000 deceased people with military ties. Unauthorised users had access from October 2025 to July 2026, until a file-sharing vulnerability was patched on 16 July. Affected individuals will receive 12 months of credit monitoring.

Sources:

- [Federal News Network](#)

Mythos-Discovered Rejetto HFS Flaw Exploited Within a Day

Horizon3 used Anthropic's Mythos model to find CVE-2026-61500 in Rejetto HFS, where session cookies are signed with a key derived from V8's Math.random(). An unauthenticated endpoint leaks raw outputs, letting the Z3 solver recover the key and forge admin cookies for code execution. VulnCheck detected exploitation within a day of disclosure, initially from a China-hosted IP address.

Sources:

- [Horizon3.ai](#)
- [The Register](#)

Threats

Warlock Ransomware Hits Water and Telecom Operators via SharePoint

Symantec attributes Warlock ransomware attacks on a water utility and a telecoms provider to China-nexus group Longlegs, which exploits SharePoint vulnerabilities and disables security software using the vulnerable K7RKScan driver. In one intrusion, the tool reached over 40 hosts within two hours and Warlock infected at least 33 machines.

Sources:

- [Symantec](#)

China-Aligned TA419 Impersonates Policymakers to Phish AI Experts

Proofpoint identified TA419 impersonating a former White House science policy official to phish AI policy experts at US think tanks and universities. A Browser-in-the-Browser kit relays genuine Microsoft sign-in traffic and captures session cookies even after multi-factor authentication succeeds.

Sources:

- [Proofpoint](#)

BPFDoor and AVERAT Implants Target Telecom Mail Appliances

Rapid7 analysed Linux implants that impersonate vendor software on South Korean and Taiwanese mail security appliances. AVERAT communicates over port 25 using SMTP, and its payloads are deleted ten seconds after launch, leaving processes running without files on disk.

Sources:

- [Rapid7](#)

Infrastructure & Exploits

Zimbra Flaw Exploited Before Public Disclosure

Microsoft tracked exploitation of Zimbra command injection flaw CVE-2026-73570 beginning before its 13 August disclosure. Attackers used a crafted email to deploy JSP web shells, escalate privileges through PAM configuration changes and move laterally using the server's SSH identity.

Sources:

- [Microsoft Threat Intelligence](#)

Fortinet Warns of Exploited FortiMail Path Traversal Zero-Day

Fortinet disclosed CVE-2026-104286, a critical FortiMail path traversal flaw with a CVSS score of 9.8 that allows unauthenticated arbitrary file writes. It affects versions 7.2 to 8.0, exploitation has been reported in the wild, and patched releases are upcoming.

Sources:

- [Fortinet](#)

Apple Patches CoreGraphics Zero-Day Reported by Meta

Apple fixed CVE-2026-86950, a CoreGraphics out-of-bounds write that may have been exploited in an extremely sophisticated attack against specific individuals. Fixes are available in iOS 26.7.1, iPadOS 26.7.1, macOS Tahoe 26.7.1 and macOS Sequoia 15.8.1.

Sources:

- [SecurityWeek](#)

Tools & Techniques

PolinRider Malware Hides Command Servers in Ethereum Transactions

SafeDep identified 35 GitHub repositories carrying the PolinRider loader, which reads Ethereum transactions from operator wallets to find command servers encoded in recipient addresses. It installs an infostealer targeting environment secrets, browser data and wallets.

Sources:

- [SafeDep](#)

Agentic Attack Chains Two Zammad Zero-Days to Breach DIVD

The Dutch Institute for Vulnerability Disclosure said an agentic AI-powered attack exploited Zammad zero-days CVE-2026-102489 and CVE-2026-102490 to hijack sessions and escalate to root. Network segmentation limited access, although volunteer data was exfiltrated.

Sources:

- [DIVD](#)

Fake ChatGPT Custom GPT Delivers Multi-Stage RAT

Huntress identified a fake Custom GPT called “Plus 5.6” that directs victims to a ClickFix-style attack triggering an eight-stage infection chain. The final remote access trojan can capture camera and microphone input, and at least 40 incidents are confirmed.

Sources:

- [Huntress](#)

Policy & Legal

Ex-US Soldier Sentenced to 70 Months for Telecom Hacking

Former US Army soldier Cameron Wagenius, known as “kiberphant0m”, was sentenced to 70 months and ordered to pay nearly \$295,000 in restitution. He breached at least 10 organisations using a tool called SSH Brute, including activity tied to the 2024 Snowflake data theft.

Sources:

- [The Record](#)

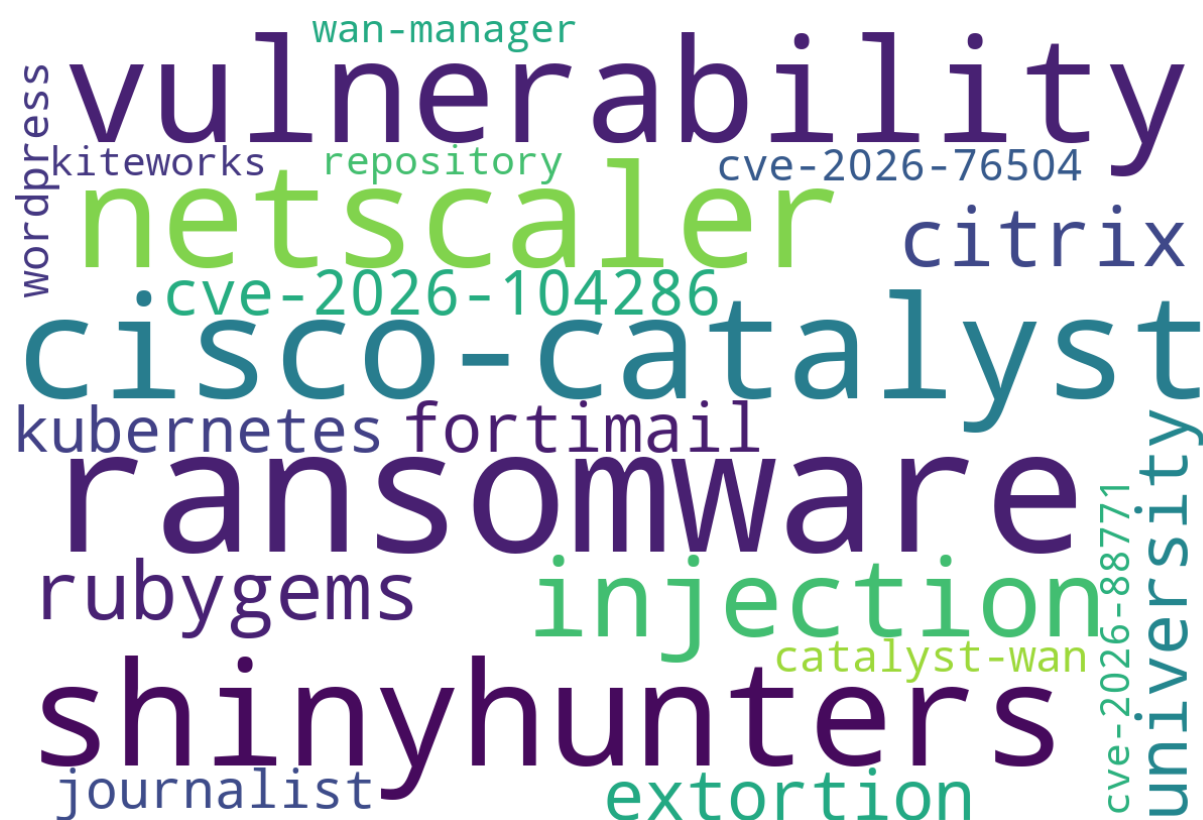
Operation KillSwitch Dismantles KillSec Ransomware Leak Site

A Dutch national known as Archduke was indicted and arrested in the UK for operating KillSec. Authorities made three provisional arrests and seized a leak site holding at least 110 terabytes of data, covering around 1,000 suspected attacks.

Sources:

- [U.S. Department of Justice](#)

Weekly Topic Distribution



Copyright and Legal Notice

© CyberSecBrief. All rights reserved.

Reproduction, redistribution, or modification of this document or its contents without explicit written permission is strictly prohibited.

Disclaimer & Terms of Use

CyberSecBrief is a personal, non-commercial project operated from Germany and is not affiliated with any company or organisation. The information provided is intended solely for general informational and educational purposes and does not constitute professional cybersecurity, legal, or financial advice. Security-related information changes rapidly; although accuracy and timeliness are sought, no guarantee is given regarding completeness, correctness, or applicability. Users must verify details with official sources or qualified professionals before making decisions.

The owner disclaims liability for any indirect, incidental, or consequential damages arising from reliance on this material. External links and third-party feeds are offered for convenience; their content, accuracy, availability, and privacy practices are outside our control and are not endorsed. Sponsored or promoted material may appear, yet inclusion does not imply endorsement.

Original content is protected by copyright. Where external material is used, appropriate attribution is provided. Reproduction of original content without prior written consent is prohibited. Content may be updated, modified, or removed at any time without notice.

This disclaimer and the Terms of Use are governed by the laws of Germany and applicable European Union regulations. Should any provision be deemed invalid, the remaining provisions shall continue in full force and effect.

Credits and Sources

CVE entries are sourced from the [CVE® Program](#), operated by [The MITRE Corporation](#), and from the [National Vulnerability Database \(NVD\)](#), maintained by the National Institute of Standards and Technology (NIST). The NVD is provided “as is” without warranty of any kind.

Definitions for APT groups are derived from the [MITRE ATT&CK® knowledge base](#), reproduced and distributed with the permission of The MITRE Corporation. © 2025 The MITRE Corporation.

All feeds and advisories are properly acknowledged and linked to their original sources where referenced, including within briefings.

Logo icon created by Ida Desi Mariana — [Flaticon](#).

Powered by [CyberFeedBites](#).

Source

This briefing is published by *CyberSecBrief* –
<https://www.cybersecbrief.com/>