

/SITREP

2026, Week 40 (28 September - 05 October 2026) | Generated 05 October 2026

Threat level: **HIGH** Trend: **rising**

Reason: three exploited Citrix NetScaler zero-days, now under mass exploitation, plus exploited FortiMail, Cisco SD-WAN and Zammad flaws, and continuing attacks on aviation, courts and healthcare.

> TOP ITEMS

- > **RED** **Citrix NetScaler ADC/Gateway: three exploited zero-days in one week.** CVE-2026-88771 and CVE-2026-88772 (CVSS v4.0 9.5 each, remote code execution) were exploited before patches existed; CVE-2026-88779 (denial of service on SAML setups) followed on 04 October. Exploitation of CVE-2026-88771 reportedly turned into mass scanning after a public proof of concept appeared, and researchers are checking whether CVE-2026-88779 also allows code execution. Action: patch both rounds, and check for compromise before upgrading because updates can erase evidence. [CISA, BleepingComputer, Help Net Security]
- > **RED** **Fortinet FortiMail CVE-2026-104286 (CVSS 9.8).** An unauthenticated path traversal allows arbitrary file writes and was exploited as a zero-day. As of 02 October no fixed build existed; Fortinet named 7.4.9, 7.6.7 and 8.0.2 as upcoming releases. Action: apply the vendor workaround (disable identity-based encryption), keep the management interface off the internet and review the published indicators. [Help Net Security, Cybersecurity Dive]
- > **RED** **Cisco Catalyst SD-WAN Manager CVE-2026-76504 (CVSS 9.8).** An unauthenticated attacker can obtain admin-level access; Cisco confirmed exploitation in September and offers no workaround. It is reportedly the eighth Cisco SD-WAN entry in CISA KEV this year. Action: upgrade to a fixed release, remove internet exposure and hunt for POST requests to URL-encoded variants of /j_security_check. [Canadian Cyber Centre, The Hacker News]
- > **RED** **Zammad zero-days used in an AI-assisted breach of DIVD.** CVE-2026-102489 (session hijack leading to code execution) and CVE-2026-102490 (local privilege escalation to root) were chained against the Dutch vulnerability-disclosure non-profit on 21 September; DIVD says the speed pointed to an agentic AI tool. DIVD advises upgrading to Zammad 7 or taking instances offline. One analyst note says version 7 does not remove the escalation flaw. [Infosecurity Magazine, Help Net Security, CSA note]
- > **AMBER** **Warlock ransomware keeps abusing SharePoint flaws.** Symantec links the China-based operator (tracked as Storm-2603 or Longlegs) to at least four recent victims in Portuguese- and Spanish-speaking countries, including a water utility and a telecom provider. In one intrusion it disabled security software on 40 or more systems before encrypting. Action: patch on-premises SharePoint and enable EDR tamper protection. [SecurityWeek, Symantec]
- > **AMBER** **Apple CoreGraphics CVE-2026-86950 (CVSS 8.8).** Apple says the out-of-bounds write may have been used in an extremely sophisticated attack on specific individuals; Meta's product security team reported it. Fixes are in iOS and iPadOS 26.7.1, macOS Tahoe 26.7.1 and macOS Sequoia 15.8.1. Action: update devices, and enable Lockdown Mode for high-risk users. [Security Affairs, Security Affairs (KEV)]
- > **GREEN** **KillSec ransomware operation dismantled.** On 30 September, Hamburg's state criminal police led Operation KillSwitch: three arrests (including a suspected 16-year-old administrator in Spain), five servers seized and at least 110 TB of stolen data secured. Authorities link the group to about 1,000 suspected attacks. [The Record, Security Affairs]

> ACTIVELY EXPLOITED VULNS (CISA KEV)

CVE	Product	Issue	KEV added	US federal due	Note
CVE-2026-88779	Citrix NetScaler ADC/GW	Memory overflow (DoS; RCE under investigation)	04 October 2026	07 October 2026	0-day SAML only [CISA, Help Net Security]
CVE-2026-88771 / -88772	Citrix NetScaler ADC/GW	Critical RCE (update)	27 September 2026	30 September 2026	0-day mass exploitation [CISA, Help Net Security]
CVE-2026-102489 / -102490	Zammad	Session fixation / improper privilege management	02 October 2026	05 October 2026	Check logs first [CISA, Infosecurity Magazine]
CVE-2026-104286	Fortinet FortiMail	Path traversal / arbitrary file write	01 October 2026	04 October 2026	0-day no patch yet [Security Affairs, CISA KEV]
CVE-2026-76504	Cisco Catalyst SD-WAN Manager	Authentication bypass (URI encoding)	30 September 2026	03 October 2026	No workaround [Canadian Cyber Centre, Security Affairs]
CVE-2026-86950	Apple CoreGraphics	Out-of-bounds write	29 September 2026	02 October 2026	Targeted attacks [Security Affairs, CISA KEV]

Sources: CISA KEV catalogue (entries checked on 05 October 2026), linked vendor and CISA notices. CISA marks ransomware use as unknown for the entries checked and requires forensic triage under BOD 26-04.

> RECOMMENDED ACTIONS FOR OPERATORS

- > **24 hours:** inventory NetScaler, FortiMail, Cisco SD-WAN Manager and Zammad; upgrade or mitigate, and take management interfaces off the internet. [[CISA](#), [Help Net Security \(FortiMail\)](#), [Canadian Cyber Centre](#), [Help Net Security \(Zammad\)](#)]
- > **72 hours:** on NetScaler, run Citrix's compromise check via NetScaler Console, treating its "nobody process" result with care, and preserve evidence before upgrading; on SD-WAN Manager, search logs for URL-encoded /j_security_check requests; roll out the Apple 26.7.1 updates. [[Help Net Security](#), [The Hacker News](#), [Security Affairs](#)]
- > **This week:** patch on-premises SharePoint and enable EDR tamper protection; check Oracle PeopleSoft systems are patched for CVE-2026-35273; require MFA on all remote access. [[SecurityWeek](#), [Help Net Security](#)]

> ATTACKS AND INCIDENTS

Victim	Sector / region	What happened	Impact
Air Traffic and Navigation Services	Aviation, South Africa	Ransomware-linked malware found in OT behind weather services; forensic help sought; possible data theft under review [SC_Media]	Operational
Arizona court system	Government, US	Phishing led to copied backups: 150,000+ foster care review reports, protective-order records, and possibly 1M+ people in a court-debt programme [Malwarebytes , FOX_10]	Sensitive data
FBI job portals	Government, US	Offline after ShinyHunters claimed a breach via a PeopleSoft zero-day; FBI confirms it is investigating, claims unverified [Cybersecurity Dive , BleepingComputer]	Claimed
Times Car (Park24)	Mobility, Japan	Up to 6.6M accounts affected, including about 1.6M identity documents; card data and recoverable passwords reportedly not exposed [SC_Media , Hackread]	6.6M accounts
Fakturownia	Invoicing SaaS, Poland	Attacker exploited a vulnerability and copied much of the database (password hashes, tokens, bank details); 600,000+ businesses use the platform; national e-invoicing system reported unaffected [The Record , PurePC (Polish)]	Supply chain
Enel-Med	Healthcare, Poland	Intrusion detected 24 September; about 3% of the patient base may be affected; clinics operating normally [Prawo.pl (Polish) , PAP via xyz.pl (Polish)]	Confirmed
Dutch Institute for Vulnerability Disclosure	Non-profit, Netherlands	Breached on 21 September through Zammad zero-days; volunteer contact data taken, spread contained by segmentation [Infosecurity Magazine , Security Affairs]	Confirmed
Keio Corporation; Tokyo Metro	Rail, Japan	Keio reported ransomware on 26 September with no impact on rail operations; Tokyo Metro said 59,000 loyalty-scheme email addresses were accessed [Infosecurity Magazine]	Confirmed

> THREAT ACTORS

Actor / cluster	Target	Activity this week	Relevance
Warlock (Storm-2603 / Longlegs, China-based)	Utilities, telecom, government, education	SharePoint exploitation, security tools disabled, payload staged via SYSVOL [SecurityWeek , The Record]	High
Unattributed NetScaler exploiters	Internet-facing edge devices, global	Targeted zero-day use, then mass exploitation; Citrix has not named an actor [The Next Web , Help Net Security]	High
ShinyHunters / ScatteredLapsussHunters	Enterprise, government	Claimed FBI portal breach; renewed PeopleSoft exploitation reported by Mandiant; Dutch police arrested a 24-year-old alleged leader, which the group denies [Help Net Security , CyberScoop , IT-Daily (German)]	Medium
"Fingerprint" (reported)	Polish healthcare and SaaS	Polish outlets link the actor to the Fakturownia theft and earlier MyDr and Medyc leaks [money.pl (Polish) , PurePC (Polish)]	Medium
KillSec (ransomware-as-a-service)	Global, cloud storage and exposed software	Infrastructure seized, three arrests; Europol says the group used AI to build infrastructure [The Record , Security Affairs]	Disrupted

> GERMANY AND EU FOCUS

- > Hamburg's state criminal police and prosecutor led Operation KillSwitch; German authorities count at least 70 attacks linked to KillSec in Germany, 18 with a Hamburg connection. [[IT-Daily \(German\)](#), [Security Affairs](#)]
- > Luxembourg's financial regulator CSSF told supervised entities that unauthenticated code execution on NetScaler counts as a major ICT-related incident that must be reported under DORA or national rules. [[CSSF](#)]
- > The Netherlands' DIVD is scanning for exposed Zammad instances and notifying owners after its own breach; Zammad is published by Zammad GmbH. [[Security Affairs](#), [CISA](#)]
- > Poland sees a run of data-theft incidents, now Fakturownia and Enel-Med after the MyDr leak affecting about 19 million people; CERT Polska and the data-protection authority are involved. [[The Record](#), [Prawo.pl \(Polish\)](#)]

> TOP NEWS

- > [BleepingComputer](#): Citrix patches the NetScaler SAML zero-day while researchers probe a possible code-execution route.
- > [Help Net Security](#): NetScaler exploitation escalates into mass attacks after a public proof of concept.

- > [SecurityWeek](#): Warlock widens SharePoint attacks on critical infrastructure.
- > [The Record](#): police disrupt KillSec and arrest its suspected teenage leader.
- > [Cybersecurity Dive](#): Fortinet warns of an exploited FortiMail flaw without a patch.
- > [Security Affairs](#): an AI agent chained two Zammad zero-days to take over DIVD systems in seconds.

> WATCHLIST

- > Whether researchers confirm code execution for CVE-2026-88779. [[BleepingComputer](#)]
- > Release of the FortiMail fixes (7.4.9, 7.6.7, 8.0.2) and further exploitation before then. [[Cybersecurity Dive](#)]
- > A formal Zammad advisory and a fix for the privilege-escalation flaw, which one analysis says persists in version 7. [[CSA note](#)]
- > Possible data leaks after ShinyHunters' ultimatum to the FBI, and further PeopleSoft attacks. [[Help Net Security](#)]

Sources:

Official / vulnerability data: Australian Cyber Security Centre, BSI CERT-Bund WID, Canadian Centre for Cyber Security, CERT-EU, CERT-In, CISA KEV, CNNVD, CNVD, CVE.org, ENISA EUVD, Exploit-DB, FSTEC BDU, Israel National Cyber Directorate, NCSC NZ, NCSC UK, NVD

Researchers / vendors: Check Point Research, DIVD CSIRT, Kaspersky Securelist, Microsoft Security Blog, Positive Technologies, Symantec Threat Intelligence, watchTower Labs

News: Anquanke, Anti-Malware.ru, Ars Technica Security, Black Arrow Cyber, BleepingComputer, Borns IT- und Windows-Blog, Computer Weekly, CSO Online, CTech, Cyber Daily, CyberScoop, Dark Reading, DataBreachToday, FreeBuf, Golem.de, heise security, Help Net Security, Infosecurity Magazine, IT World Canada, IT-Daily, iNews, konbriefing.com, Krebs on Security, Risky Business News, SC Media, Schneier on Security, Secrss, Security Affairs, Security-Insider, SecurityLab.ru, SecurityWeek, TechCrunch Security, The Cyber Express, The Cyber Wire, The Hacker News, The Record, The Register, WIRED Security, Xakep.ru

Claims by press and vendors; claimed breaches (ShinyHunters) are unverified. Compiled from public sources only. Prepared with the assistance of a large language model. Provided without warranty, and all liability is excluded to the extent permitted by law.



m



PGP key

[january1073](#)