

/SITREP

2026, Week 41 (06 - 12 October 2026) | Generated 12 October 2026

Threat level: HIGH **Trend: stable**

Reason: exploitation of a critical Atlassian Data Center flaw within hours of a public proof of concept, the FortiBleed firewall credential campaign with admin lockouts, continuing NetScaler and FortiMail exposure, and a joint advisory and takedown against China-linked Flax Typhoon.

> TOP ITEMS

- > **RED** **Atlassian Data Center CVE-2026-21589 (CVSS 4.0 9.3)**. An unauthenticated arbitrary file access flaw affects eight self-hosted products, including Jira, Confluence, Bitbucket and Crowd; Atlassian disclosed it on 05 October. The attacker must know the file path, but watchTowr showed that in Crowd-integrated setups plaintext credentials can be read and used to create admin accounts. Previdian saw exploitation attempts about two hours after the public proof of concept on 06 October. Action: upgrade, or remove instances from the internet and apply Atlassian's rewrite rules, then review access logs. [[watchTowr](#), [BleepingComputer](#), [CERT-EU via Lovguiden](#)]
- > **RED** **FortiBleed credential campaign**. A joint FBI and Secret Service advisory (06 October) describes an ongoing campaign, not a new CVE, against internet-facing FortiGate firewalls and SSL VPN gateways. SOCRadar verified 86,644 compromised devices in 194 countries; attackers crack stolen password hashes offline, add or delete admin accounts, and in some cases lock owners out. Access is reportedly sold to INC/Lynx and Payload ransomware affiliates. Action: take admin interfaces off the internet, reset all admin and VPN credentials, enforce phishing-resistant MFA and review accounts and API keys. [[FBI and Secret Service advisory](#), [Help Net Security](#)]
- > **RED** **Citrix NetScaler (update)**. watchTowr reproduced CVE-2026-88779 as a denial-of-service bug only; CISA says attackers can use it to force a reboot that activates code planted through CVE-2026-88771. eSentire reported on 06 October at least four exploitation clusters using web shells and backdoor accounts. Action: install the latest builds and hunt for web shells and unknown accounts. [[CISA alert](#), [SecurityWeek](#), [The Hacker News](#)]
- > **AMBER** **Flax Typhoon and Integrity Technology Group**. On 08 October agencies from seven countries named the China-based company as enabling actors consistent with Flax Typhoon, Ethereal Panda and Red Juliett. The DOJ and FBI seized seven domains tied to the MicroScan scanner and FishHub spear-phishing tool, and CISA added five of the eight flaws the advisory lists to KEV. The agencies note that not all activity may be linked to the company. Action: patch edge and legacy software and check logs against the published indicators. [[CISA](#), [BleepingComputer](#)]
- > **AMBER** **SonicWall SMA 1000 CVE-2026-102255 (CVSS 10)**. A pre-authentication SSRF in the Work Place interface, disclosed on 07 October; SonicWall sees no evidence of exploitation yet. It is the third 10.0 flaw in this interface in about three months, and earlier ones were exploited. Fixed builds are 12.4.3-03670 and 12.5.0-03082; there is no workaround. Action: verify the full build on every appliance and keep management off the internet. [[Network World](#), [Help Net Security](#)]
- > **AMBER** **Country-code registries hijacked**. Google disclosed on 06 October that attackers took over the .gh, .sl and .as registries, changed DNS records and obtained HTTPS certificates for Google domains and others. The certificates were revoked and Chrome blocks them. Action: owners of domains under these suffixes should review certificate transparency logs and set restrictive CAA records. [[Help Net Security](#), [The Register](#)]
- > **GREEN** **Arrests in ransomware and extortion cases**. Japan handed a suspected core Qilin member to Germany, announced on 07 October after months of infiltration by North Rhine-Westphalia's criminal police. The FBI announced a further ShinyHunters-linked arrest on 09 October, and a suspect known as Rey is reportedly detained in Jordan. Both groups are still operating. [[SecurityWeek](#), [BleepingComputer](#)]

> ACTIVELY EXPLOITED VULNS (CISA KEV)

CVE	Product	Issue	KEV added	US federal due	Note
CVE-2015-3306	ProFTPD	Improper access control (file read and write)	08 October 2026	11 October 2026	Flax Typhoon use [CISA KEV , The Hacker News]
CVE-2016-3081	Apache Struts	Command injection (Dynamic Method Invocation)	08 October 2026	11 October 2026	Flax Typhoon use [CISA KEV , The Hacker News]
CVE-2021-3199	ONLYOFFICE Docs	Path traversal (RCE)	08 October 2026	11 October 2026	Flax Typhoon use [CISA KEV , The Hacker News]
CVE-2015-5477	ISC BIND	Reachable assertion (DoS)	08 October 2026	11 October 2026	Flax Typhoon use [CISA KEV , The Hacker News , Security Affairs]

CVE-2023-22894	Strapi	Cleartext storage of sensitive data	08 October 2026	11 October 2026	End-of-life product [CISA_KEV, The Hacker_News]
CVE-2026-88779 (update)	Citrix NetScaler ADC/GW	Memory overflow, DoS only per watchTower	04 October 2026	07 October 2026	Can force reboots [CISA, SecurityWeek]
CVE-2026-104286 (update)	Fortinet FortiMail	Path traversal / file write	01 October 2026	04 October 2026	Fixed builds unconfirmed [CSA Singapore, CISA_KEV]
CVE-2026-102489 / -102490 (update)	Zammad	Session fixation / privilege escalation	02 October 2026	05 October 2026	7.2.0 hardens first only [Zammad community, CISA]

Sources: [CISA KEV catalogue](#) (entries checked on 12 October 2026), linked vendor and CISA notices. CISA marks ransomware use as unknown for the entries visible in the catalogue snapshot; forensic triage under BOD 26-04 is required for some (Strapi, FortiMail, Zammad) and not for others (BIND, NetScaler CVE-2026-88779).

> RECOMMENDED ACTIONS FOR OPERATORS

- > **24 hours:** remove self-hosted Atlassian instances and Fortinet admin interfaces from the internet, upgrade Atlassian, and reset all FortiGate admin and VPN credentials. [[watchTower](#), [FBI and Secret Service advisory](#), [CISA alert](#)]
- > **72 hours:** verify SonicWall SMA 1000 builds, apply the FortiMail workaround (disable identity-based encryption, restrict management) and hunt for compromise, and check repositories for the malicious workflows. [[Network World](#), [CSA Singapore](#), [The Hacker News](#)]
- > **This week:** prepare for Microsoft Patch Tuesday on 13 October, update Chrome to 155, and patch the older Struts, ProFTPD, BIND, ONLYOFFICE and Strapi exposures named in the Flax Typhoon advisory. [[Help Net Security](#), [eSecurityPlanet](#), [CISA](#)]

> ATTACKS AND INCIDENTS

Victim	Sector / region	What happened	Impact
IDC Frontier (IDCF Cloud)	Cloud provider, Japan	Ransomware on 07 October took down East Japan Region 1; reports put the affected customers, including local governments, at 495; entry point and data theft not yet disclosed [BleepingComputer , Tech Insider]	Operational
ASOS	Retail, UK	Unauthorised app notification on 06 October claimed a Snowflake compromise; ASOS says stolen employee credentials reached third-party platforms and basic personal data was exposed; the "Xuanye group" claim of wider theft is unverified [BleepingComputer , Help Net Security]	Confirmed
Central Population Register (CPR)	Government, Denmark	A private firm's legitimate access was misused; names, addresses and CPR numbers of about 8.8M people exposed, with 14M+ lookups reported; protected-address records not affected [The Register , The Next Web]	8.8M people
FBI jobs portal (update)	Government, US	FBI says a contractor failed to apply a security patch on a third-party-managed platform and removed it; Reuters reportedly named Oracle PeopleSoft and Accenture; ShinyHunters' 2 to 3 TB claim is unverified [Nextgov , CSO Online]	Confirmed

> THREAT ACTORS

Actor / cluster	Target	Activity this week	Relevance
Integrity Tech-linked (Flax Typhoon, China)	Critical infrastructure, global	Named in a seven-nation advisory; seven domains seized; botnet, VPN and living-off-the-land tradecraft [CISA , Help Net Security]	High
FortiBleed access brokers (unattributed)	FortiGate firewalls and VPNs	Credential stuffing and hash cracking at scale; lockouts; access passed to INC/Lynx and Payload affiliates [FBI and Secret Service advisory , Help Net Security]	High
ShinyHunters	Enterprise, government	Further arrests reported; the group says it will not publish FBI data; a new leak site appeared [BleepingComputer , Help Net Security]	Medium
Qilin (ransomware-as-a-service)	Global, incl. Germany	Suspected core member extradited to Germany; German officials count about 150 attacks in Germany; group still active [SecurityWeek , ZDFheute (German)]	Medium
UAC-0099 (Russia-aligned)	Ukraine, Windows hosts	ESET traced about two years of changes to the MATCHBOIL downloader that installs a spying backdoor [Help Net Security]	Medium

> GERMANY AND EU FOCUS

- > North Rhine-Westphalia's criminal police and cybercrime prosecutors infiltrated Qilin and now hold a 28-year-old Russian suspect extradited from Japan; the state interior minister counts about 150 Qilin attacks in Germany. [[ZDFheute \(German\)](#), [SecurityWeek](#)]
- > Denmark's population register breach exposed about 8.8M records; the Danish Data Protection Agency has opened a case and police are investigating. [[Help Net Security](#), [The Register](#)]
- > CERT-EU issued advisory 2026-015 on the Atlassian flaw on 06 October; heise reported the first attacks on 08 October. [[CERT-EU via Lovguiden](#), [heise security \(German\)](#)]
- > Modat and the Dutch NCSC found 8,547 internet-facing control systems at wind and solar parks across 35 countries in and around the EU, including a turbine page with a Stop button. [[Help Net Security](#)]

> TOP NEWS

- > [The Hacker News](#): over 500 accounts planted credential-stealing GitHub Actions workflows in tens of thousands of repositories since 07 October.

- > [eSecurityPlanet](#): Chrome 155 fixes 247 flaws, four critical, with no exploitation reported.
- > [Help Net Security](#): the owner of ransomware recovery firm MonsterCloud is charged with secretly paying attackers while overbilling clients.
- > [Help Net Security](#): the FBI and French police seize two sites selling stolen intimate images and arrest the suspected administrator.

> WATCHLIST

- > **RESOLVED** CVE-2026-88779 is a denial-of-service bug, not code execution, according to watchTower, though it can force reboots. [[SecurityWeek](#), [CISA alert](#)]
- > **OPEN** FortiMail fixes (7.4.9, 7.6.7, 8.0.2) are still unconfirmed; a 06 October advisory still says to update once available. [[CSA Singapore](#)]
- > **OPEN** Zammad says 7.2.0 hardens CVE-2026-102489, but no fix is confirmed for the privilege-escalation CVE-2026-102490. [[Zammad community](#)]
- > **RESOLVED** ShinyHunters says it will not publish the FBI data and the FBI traced the breach to a missed contractor patch. [[Nextgov](#), [Help Net Security](#)]
- > Microsoft Patch Tuesday on 13 October, after September's record 973 CVEs, with Chrome 156 also due. [[Help Net Security](#)]
- > Whether CISA adds CVE-2026-21589 to KEV. [[SecurityWeek](#)]
- > Recovery and attribution at IDCf Cloud. [[BleepingComputer](#)]
- > Further ShinyHunters arrests and any Flax Typhoon infrastructure rebuild. [[BleepingComputer](#), [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 (the "Xuanye group" at ASOS, ShinyHunters at the FBI) 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](#)