



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

5 October 2026

Vulnerabilities

Microsoft Pushes New Exchange V2 Update After Discovering New Security Flaw

Cyber Security News - 03 October 2026 15:59

Microsoft has released September 2026 V2 security updates to fix an Exchange Server flaw that lets authenticated attackers access other users' mailboxes within the same organization. Tracked as CVE-2026-96940, the vulnerability could expose email messages and attachments, making it a serious concern for businesses running Exchange on-premises.

Citrix patches NetScaler SAML zero-day exploited in attacks

BleepingComputer - 04 October 2026 18:58

Citrix has released emergency updates for a new NetScaler denial-of-service vulnerability tracked as CVE-2026-88779 that has been exploited in zero-day attacks, with researchers investigating whether it can also be exploited for remote code execution. [...]

GitLab warns of critical RCE vulnerability in AI Gateway service

BleepingComputer - 02 October 2026 13:20

GitLab warned customers today to immediately patch a critical AI Gateway vulnerability that could let attackers run arbitrary commands on vulnerable instances. [...]

Dell asks admins to patch max severity CSM flaws as soon as possible

BleepingComputer - 02 October 2026 09:37

Dell has patched two maximum severity vulnerabilities in the Container Storage Modules (CSM) that connect Dell enterprise storage arrays to Kubernetes environments. [...]

Critical FortiMail Zero-Day Flaw Exploited in Attacks Allows Unauthenticated Arbitrary File Writes

The Hacker News - 02 October 2026 12:19

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), on Thursday, added a critical security flaw impacting Fortinet FortiMail to its Known Exploited Vulnerabilities (KEV) catalog, following reports of active exploitation.

Fortra Patches Critical Vulnerabilities in BoKS

SecurityWeek - 03 October 2026 12:34

The bugs could lead to authentication bypass, shell command execution, and memory corruption.



Threat actors and malware

[Cling Malware Masquerades as Google STUN Traffic to Control Compromised IoT Devices](#)

Cyber Security News - 05 October 2026 08:43

Cling malware is turning compromised internet-connected devices into a botnet while disguising its control traffic as replies from Google's public STUN service. The technique makes attacker instructions look like routine communications used by applications to connect across network boundaries.

[Warlock ransomware breach SharePoint in water, telecom operator attacks](#)

BleepingComputer - 02 October 2026 15:33

The China-linked ransomware group Warlock targeted a water utility, a telecom provider, a regional government body, and a university by exploiting SharePoint vulnerabilities to gain initial access. [...]

[Warlock Ransomware Still Exploits Year-Old SharePoint Flaws to Hit Critical Infrastructure](#)

Security Affairs - 04 October 2026 08:49

Warlock ransomware continues to exploit unpatched SharePoint flaws to breach water utilities, telecoms, governments, and universities worldwide.

[Antino Backdoor Lets China-Linked UAT-11587 Turn Microsoft 365 Into a C2 Channel](#)

Security Affairs - 03 October 2026 10:26

Cisco Talos details UAT-11587, a China-linked group using the Antino backdoor and Microsoft 365 as cover to spy on Asian governments. Cisco Talos has been tracking a cluster of espionage activity since September 2025 that it calls UAT-11587, and by July 2026 the group had hit at least 16 government and policy organizations across eight [...]

[China-Aligned TA419 Targets U.S. AI Policy Experts With Microsoft AitM Phishing](#)

The Hacker News - 04 October 2026 13:50

A new China-nexus cyber espionage group known as TA419 has been attributed to multiple credential phishing campaigns targeting artificial intelligence (AI) experts working for U.S. think tanks, universities, and legal sector organizations.

[macOS Users Targeted by Fake Zoom Installer Carrying CloudSyncD Backdoor](#)

SecurityWeek - 02 October 2026 14:15

The dropper "carries a complete universal Mach-O inside itself, roughly 756 KB in the development build, and extracts it at runtime.