



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

1 October 2026

Vulnerabilities

Cisco warns of new SD-WAN zero-day exploited in attacks

BleepingComputer - 30 September 2026 11:46

Cisco released security updates to address a critical zero-day in the Catalyst SD-WAN Manager (tracked as CVE-2026-76504) that attackers are actively exploiting to escalate to admin privileges.

Attackers Exploit Zimbra Flaw to Deploy Web Shells and Harvest Authentication Secrets

The Hacker News - 30 September 2026 23:16

Threat actors have weaponized a now-patched security flaw in Zimbra Collaboration Suite (ZCS) to deploy web shells and access mailbox data, according to findings from the Microsoft Security Research team.

Apple Patches CoreGraphics Zero Day Exploited in Attacks

Infosecurity Magazine - 30 September 2026 09:45

Apple has patched CVE-2026-86950, a zero-day bug in the iOS CoreGraphics engine.

WatchGuard fixes critical Fireware OS flaw allowing remote code execution

Security Affairs - 30 September 2026 20:29

WatchGuard has released security updates for Fireware OS that address 15 vulnerabilities, including a critical code injection flaw, tracked as CVE-2026-86131 (CVSS score of 9.2).

TeamViewer urges users to patch severe flaws "as soon as possible"

BleepingComputer - 30 September 2026 09:25

Remote access software company TeamViewer warned customers on Tuesday to immediately patch a set of high-severity vulnerabilities affecting its client and host software.

Citrix NetScaler Post-Exploitation Payload Creates Superuser, Maps Web Shell to CSS-Like URLs

The Hacker News - 01 October 2026 11:05

Threat actors have been observed exploiting a critical pre-authentication command injection vulnerability in Citrix NetScaler ADC and NetScaler Gateway to drop web shells and attempt theft of configuration data.



Scottish
Cyber
Coordination
Centre

Chrome, Firefox Updates Patch Over 100 Vulnerabilities

SecurityWeek - 30 September 2026 13:16

Some of the flaws could allow remote attackers to execute arbitrary code or escape the browser sandbox.

Threat actors and malware

Microsoft to block Entra ID script injection attacks starting October

BleepingComputer - 30 September 2026 10:37

Microsoft has reminded customers that the Entra ID authentication system will get better protection against external script injection attacks starting next month.

WHIPSHOT and SLAPSHOT: the tools behind an active Citrix NetScaler campaign

Security Affairs - 30 September 2026 08:25

Mandiant and GTIG detail active exploitation of a Citrix NetScaler zero-day, deploying custom web shells WHIPSHOT and SLAPSHOT for root access.

Attackers Abuse MSP360 to Deploy ScreenConnect in Dual-RMM Phishing Attacks

The Hacker News - 30 September 2026 23:02

Microsoft has warned of phishing campaigns distributing an installer for the MSP360 Remote Monitoring and Management (RMM) software under the guise of meeting invitations, PDF-themed lures, software update prompts, and other social-engineering content.

US-Focused CSuite Phishing Steals Microsoft 365 Sessions and Deploys RMM Tools for Remote Access

The Hacker News - 30 September 2026 17:15

ANY.RUN researchers traced a US-focused CSuite phishing campaign across 351 sandbox analyses, with 51% of submissions coming from the United States. Technology, manufacturing, government, and consulting organizations showed the highest exposure.

Russian APT Star Blizzard Uses 'RedFlick' Infection Chain in Recent Attacks

SecurityWeek - 30 September 2026 11:59

The state-sponsored group has launched larger-scale phishing campaigns to deploy the CosmicPulse backdoor.