Periculo Threat Report - 10.11.25

This week's report: A critical Cisco update, widespread exploitation of Microsoft WSUS with emergency patching guidance, and a high-severity AMD CPU issue that can weaken cryptography. Below, let's look at what happened, why it matters, and what to do next...

Apple WebKit vulnerabilities discovered by Google's Big Sleep

Apple released security updates addressing five WebKit flaws (including buffer overflow and use-after-free issues) credited to Google's AI-assisted vulnerability discovery effort "Big Sleep." While Apple did not flag in-the-wild exploitation for these specific CVEs, WebKit sits at the heart of Safari and many in-app browsers, making rapid updates important. The patches shipped as part of iOS/iPadOS 26.1, macOS Tahoe 26.1 and Safari 26.1. Given the ubiquity of iOS devices among clinicia...

Clinicians frequently access EPR portals, imaging viewers, and email from iPhones and iPads. Unpatched WebKit bugs enable credential theft or session hijacking via malicious pages, risking access to patient and corporate systems.

Recommendations:

- Push iOS/iPadOS/macOS and Safari 26.1 updates to managed fleets; verify compliance in MDM.
- Enforce phishing-resistant MFA on all SaaS/EPR access to reduce impact of browser compromise.
- Restrict risky domains via DNS/web filtering; monitor for abnormal mobile sign-ins.

Cisco Unified Contact Center Express critical RCE and auth bypass

Cisco disclosed multiple critical flaws in Unified Contact Center Express (UCCX) that allow unauthenticated remote attackers to upload files, bypass authentication, execute commands and potentially gain root. There are no workarounds; fixed software is available and should be deployed immediately. Related advisories also cover other Cisco contact-centre components.

Many companies rely on Cisco contact-centre workflows for patient access and clinical operations. Remote code execution on UCCX risks call-handling disruption, data exposure, and a potential pivot deeper into clinical networks.

Recommendations:

- Patch UCCX to Cisco's fixed releases without delay and restrict management interfaces.
- Review exposure of Java RMI and related services; block unnecessary external access.
- Monitor for anomalous script execution and privilege escalation on UCCX hosts.
- Validate backups and roll-back plans before upgrades.

Microsoft WSUS RCE (CVE-2025-59287)

A critical unauthenticated RCE in Windows Server Update Services (WSUS) is being exploited. Microsoft shipped out-of-band updates; security teams and researchers report scanning and compromises against internet-exposed WSUS and internal targets. CISA added the CVE to KEV and set patch deadlines for U.S. agencies. UK organisations should treat this as actively exploited.

Compromising WSUS can deliver malicious updates at scale across an estate, enabling rapid lateral movement and ransomware staging in hospitals and suppliers.

Recommendations:

- Apply Microsoft's out-of-band updates and reboot WSUS servers.
- Block inbound 8530/8531 from untrusted networks; do not expose WSUS to the internet.
- Hunt for suspicious child processes of WSUS/IIS, and review update approvals for anomalies.
- If immediate patching is impossible, temporarily disable the WSUS role.

AMD Zen 5 RDSEED failure weakens randomness (AMD-SB-7055 / CVE-2025-62626)

AMD confirmed a high-severity issue on Zen 5 CPUs where the RDSEED instruction can return zero while signalling success in 16/32-bit forms, risking generation of predictable cryptographic values. AMD has published mitigations and timelines for microcode/AGESA updates; EPYC fixes are landing first, with desktop/workstation updates slated by late November.

Weak randomness can undermine TLS, VPN, SSO tokens and software-update signing in clinical apps and back-office systems. Mixed estates (on-prem and cloud) should verify CPU families and crypto dependencies.

Recommendations:

- Prefer 64-bit RDSEED or software RNG fallback until microcode is applied.
- Track OEM BIOS/firmware releases aligned to AMD's schedule; plan maintenance windows.
- Re-issue long-lived keys generated on affected systems where risk is material.

That's all for this week - prioritise Cisco UCCX patching and WSUS hardening, and schedule AMD firmware updates if you run Zen 5.

Speak with our team about Periculo Threat Intelligence and targeted remediation support.