# Periculo Threat Report - 03.11.25

Compiled by Craig Pepper

## Windows Server WSUS remote code execution (CVE-2025-59287) under active exploitation

Microsoft released out-of-band updates for a critical WSUS bug (CVE-2025-59287) that allows unauthenticated remote code execution via insecure deserialisation. Exploitation has been observed in the wild. CISA added the flaw to the KEV catalogue and directed federal agencies to patch swiftly. Thousands of internet-exposed WSUS instances remain visible, underscoring the risk of mass exploitation if servers remain unpatched or accessible on default ports.

NHS and private health estates commonly use WSUS for controlled Windows updates. Compromise can provide adversaries with domain-level footholds and a software-supply vector to push malicious updates to endpoints.

**Recommendations:**

- Patch all WSUS servers immediately; follow Microsoft's out-of-band guidance and reboot.
- Restrict WSUS to internal networks; block 8530/8531 externally; enforce TLS and authentication.
- Hunt for suspicious WSUS admin actions and unexpected client approvals; review server logs.
- Validate endpoint update chains and EDR coverage on critical clinical workstations.

## Chrome zero-day activity linked to commercial spyware vendor

New analyses tie earlier Chrome zero-day exploitation (CVE-2025-2783) to the Italian spyware vendor Memento Labs. Exploits were used to deliver surveillance tools via a sandbox-escape chain. While the original patches landed months ago, continued interest highlights browser chains as espionage vectors.

Clinical and admin staff rely on browsers for cloud EHR portals and email. A browser-level exploit can bypass endpoint controls and enable credential theft or session hijack.

**Recommendations:**

- Enforce rapid Chrome updates; verify latest stable version across managed fleets.
- Lock down extensions; disable developer mode and restrict sideloading.
- Require phishing-resistant MFA for all clinical and admin SaaS access.

Focus this week on remediating WSUS servers, tightening browser controls, and staying close to firmware and microcode advisories. Blend technical controls with prepared communications plans to blunt extortion pressure.

*Contact us to learn more about our Threat Intelligence Service.*