Periculo Threat Report - 20 October 2025

Compiled by Craig Pepper

This week's report: With urgent security updates required for Microsoft and Veeam, a major health data breach, and a supply-chain risk at F5. Organisations must take immediate, informed action to safeguard systems and protect data.

Microsoft October 2025 patches (175 CVEs; 3 exploited, 3 publicly disclosed)

NHS England flagged Microsoft's October Patch Tuesday: 175 vulnerabilities, with three under active exploitation and three publicly disclosed. This drop includes fixes across Windows client/server and Azure services. Notably, Windows 10 reached end-of-life on 14 October 2025, making this the final security update for that platform. NHS urges rapid patching and directs organisations to Microsoft's release notes for impacted components and CVEs. With exploitation confirmed for select issues, defenders should prioritise updates on internet-exposed systems, remote access services, and high-privilege endpoints, then proceed across the estate in waves aligned to clinical risk.

Clinical ops run on Windows endpoints and servers. Known-exploited bugs are a fast track to initial access or privilege escalation, risking EHR downtime and data loss. Windows 10 EoL also raises exposure for legacy devices that continue running unsupported builds.

Recommendations:

- Patch immediately per Microsoft October 2025 guidance; prioritise internet-facing and privileged systems.
- Plan/accelerate Windows 11 migration where Windows 10 persists.
- Validate backups and rollback plans before large patch waves.

Veeam Backup & Replication / Windows Agent - critical fixes (RCE/LPE)

NHS England issued an alert for Veeam updates addressing three vulnerabilities, including two authenticated RCEs in Backup & Replication (CVSS 9.9) and one LPE in the Windows Agent. Veeam warns that unsupported versions are likely affected and should be considered vulnerable. Given the central role of Veeam in backup and recovery, compromised backup infrastructure enables ransomware actors to corrupt snapshots, delete restore points, and accelerate impact. Organisations should patch to the versions in Veeam KB4771 and treat exposed or unsupported instances as incident-response priorities.

Backups are your last line of defence. If attackers control Veeam, recovery becomes unreliable and ransom pressure rises. Healthcare's intolerance for downtime makes resilient backups non-negotiable.

Recommendations:

- Patch per KB4771; remove/upgrade unsupported builds.
- Lockdown management interfaces; restrict to trusted admin networks.
- Require MFA for Veeam consoles; monitor for job tampering/deleted restore points.

F5 confirms internal network compromise; source code & vuln details stolen

NHS England raised severity to High after F5 confirmed a state-sponsored actor maintained long-term

access to its internal network and exfiltrated BIG-IP source code and undisclosed vulnerability details. F5 says there's no evidence of code-pipeline tampering or customer exploitation, but the theft increases future exploit risk. NHS and NCSC advise identifying all F5 assets, updating to supported versions, removing internet-exposed management interfaces, and reviewing hardening guides and threat-hunting steps from F5. Treat this as a supply-chain risk and monitor for targeted exploitation attempts.

BIG-IP appliances sit on the front-door of many hospital networks and supplier services. Stolen internals can speed exploit development, so proactive hardening and version currency are critical to keep patient-facing apps and APIs safe.

Recommendations:

- Inventory all F5 devices; update to latest supported releases; replace EoS hardware.
- Do not expose management interfaces to the internet; enforce MFA/VPN.
- Pull key F5 logs into your SIEM; retain for 180 days; hunt per F5/NCSC guidance.

SimonMed Imaging breach - 1.2M patient records exposed (Medusa)

US imaging provider SimonMed confirmed a breach affecting 1.2 million patients after criminals exfiltrated data between 21 Jan and 5 Feb 2025. Medusa claimed responsibility, posting samples and demanding $1 million to delete ~212 GB of data. While outside the UK, the scale and the nature of exposed records (IDs, medical reports, payment details) are highly relevant to digital health globally. TechRadar's report cites official filings and breach notices; affected individuals are being offered identity protection. UK organisations should note the extortion playbook and vendor-risk lessons.

Imaging networks and vendors hold highly sensitive data. Even indirect exposure (via a supplier) can trigger regulatory scrutiny and reputational harm. Prepare comms and safeguarding routes for patient-facing extortion fallout.

Recommendations:

- Tighten vendor-risk reviews (DSPT alignment, incident clauses, minimum controls).
- Enforce MFA and least-privilege on third-party access to imaging/EHR systems.
- Drill breach comms and patient-notification workflows.

Patch Microsoft and Veeam first, harden/monitor F5 estates, and review data-breach communications with suppliers. If you need help prioritising.

Need a tailored threat brief for your trust or vendor ecosystem? Talk to Periculo about Threat Intelligence and rapid patch prioritisation for NHS and digital health: https://www.periculo.co.uk/threat-intelligence