06.10.2025 Threat Report

October 6, 2025

By Craig Pepper · 3 minute read

This week's Threats Report: Cisco network kit under active attack, a VMware zero-day patched after a year in the wild, and a UK nursery extortion case with lessons for any organisation holding sensitive data. Here's what to patch first and how to stay ahead.

Cisco IOS/IOS XE SNMP flaw (CVE-2025-20352) Under Active Exploitation

Cisco disclosed a high-severity vulnerability in the SNMP subsystem of IOS/IOS XE (CVE-2025-20352). An authenticated remote attacker with low privileges can trigger a denial of service; in some scenarios, exploitation may enable deeper impact depending on device configuration. CISA added the CVE to the Known Exploited Vulnerabilities (KEV) catalogue on 29 September, and NHS England issued an alert urging rapid patching and tighter SNMP exposure controls. The issue is part of Cisco's September advisory bundle and affects widely deployed routing and switching gear across enterprise networks. Given active exploitation reports, organisations should assume opportunistic scanning and prioritise upgrades and access restrictions for network management services.

NHS and private health networks depend on Cisco for core connectivity. Disrupted switches/routers can impact EHR access, imaging networks and clinical comms, risking care delays. Network-device compromise also offers attackers a beachhead for lateral movement and data interception if SNMP is exposed or weakly controlled.

Recommendations:

- Patch to Cisco fixed releases; verify versions with Cisco Software Checker.
- Restrict SNMP to management subnets; disable v1/v2c; prefer SNMPv3 with strong auth.
- Rotate SNMP/community credentials and admin accounts; audit privilege level 15.
- Monitor for anomalous SNMP traffic and unexpected device reloads.

VMware Aria Operations / VMware Tools LPE (CVE-2025-41244) Exploited, Patches Released

Broadcom released fixes for multiple VMware issues, including CVE-2025-41244, a local privilege escalation affecting Aria Operations and VMware Tools. NHS England issued a cyber alert highlighting affected versions across Aria Operations, Cloud Foundation, and Tools and urging prompt updates. Trade press and researchers note this bug has seen real-world exploitation, enabling attackers or malicious processes to escalate to root on Linux guests, useful for ransomware staging or persistence. Health workloads are frequently virtualised, so delaying patching leaves clinical and back-office systems exposed even without a hypervisor escape.

Virtual machines underpin EHR, PACS, laboratory, and admin systems. Guest-level privilege escalation can lead to data theft, service disruption, and faster ransomware impact—particularly where defence relies on guest-agent telemetry.

Recommendations:

- Patch Aria Operations/Cloud Foundation and update VMware Tools or open-vm-tools per advisory.
- Disable non-essential guest features; harden Tools configuration.
- Hunt for suspicious binaries spawned from temporary paths on Linux guests.
- Enforce least-privilege RBAC for vCenter/ESXi ops.

UK Nursery Breach

Following the breach of Kido Schools, criminals published sensitive child/family data to pressure payment, then claimed to delete the data amid public backlash. Reports indicate the group contacted parents directly to escalate pressure. An increasingly common tactic that leverages emotional distress. While not a hospital breach, the incident mirrors risks health providers face when attackers target highly sensitive records and attempt to force action through reputational damage and stakeholder panic.

Many organisations also store information of significant sensitivity. Threat actors may reach out directly to users, clients, patients, or carers, heightening distress and driving complaints, FOI requests, and unwanted media attention even where core operations remain unaffected. Robust communications plans and safeguarding protocols are critical to protect stakeholders and maintain trust.

Recommendations:

- Prepare playbooks for direct-to-patient/carer extortion (legal, comms, safeguarding).
- Enforce MFA/least privilege on third-party platforms; review contracts and DSPT alignment.
- Minimise and retain data appropriately; verify vendor controls and incident clauses.
- Train staff to recognise targeted follow-on phishing using leaked data.

New CISA & NCSC Guidance to Map and Secure OT

CISA, with the UK NCSC and partners, released joint guidance on creating and maintaining a “definitive view” of OT architecture—emphasising asset inventories, supplier risk, and defensible segmentation. NCSC also published fresh materials for OT buyers and cloud-hosted SCADA decision-making. For health estates blending IT and OT (e.g., BMS, imaging, labs), these resources offer concrete steps to improve visibility and reduce blast radius.

Many organisations operate mixed IT/OT networks where poor visibility hinders incident response. Establishing an accurate OT asset map supports network segmentation, supplier assurance, and faster recovery during outages or ransomware events.

Recommendations:

- Build/maintain an OT asset inventory and data model; map interconnections.
- Bake security-by-design into OT procurement; use NCSC buyer guidance.
- Assess cloud-hosted SCADA risks with NCSC’s checklist before adoption.