29.09.2025 Threat Report

This week, a critical zero-day vulnerability in widely used networking gear, a supply chain breach affecting NHS patients, and hidden backdoors found in Medical Patient Monitors. Let's get straight to it...

Actively Exploited Zero-Day in Cisco IOS and IOS XE Software

Cisco has disclosed a critical vulnerability (CVE-2025-20352) in its IOS and IOS XE software, which is being actively exploited. The flaw resides in the Simple Network Management Protocol (SNMP) subsystem. An unauthenticated, remote attacker can send a specially crafted SNMP packet to an affected device, causing it to reload (a denial-of-service condition) or, in some cases, allowing for remote code execution with root privileges. The vulnerability is due to a stack overflow, a classic memory corruption bug. Cisco has released patches to address the issue, but the active exploitation means many organisations could already be at risk.

Cisco networking equipment forms the backbone of many UK healthcare organisations, including NHS trusts. A successful exploit could disrupt network services, impacting access to electronic health records (EHRs), connected medical devices, and critical clinical systems, with a direct impact on patient care.

Recommendations:

- Immediately identify all vulnerable Cisco devices running IOS and IOS XE software in your environment.
- Apply the security patches provided by Cisco as a matter of urgency.
- If patching is not immediately possible, restrict SNMP access to trusted networks and monitor for any unusual SNMP traffic.
- Ensure you have a robust incident response plan in place in case of a compromise.

NHS Patient Data Breach via Third-Party Supplier

NHS Humber & North Yorkshire Integrated Care Board (ICB) has apologised for a data breach originating from a third-party supplier, NRS Healthcare. NRS, which provides wheelchair and community equipment services, suffered a cybersecurity incident where an unauthorised party gained access to its systems. The breach, which occurred earlier in the year, was found to have compromised the personal and special category data of service

users. The company has since ceased trading and is in liquidation, complicating the response and support for affected individuals.

This incident highlights the significant risks posed by the healthcare supply chain. Even with robust internal security, digital health organisations are vulnerable if their partners and suppliers have weak security postures. It underscores the need for thorough due diligence and security assessments of all third-party vendors.

Recommendations:

- Review your third-party risk management programme and ensure all suppliers with access to patient data have adequate security controls.
- Include clear data breach notification clauses in all supplier contracts.
- Conduct regular security audits of critical suppliers.
- Have a clear communication plan ready for incidents involving third-party breaches.

Hidden Backdoors Found in Medical Patient Monitors

Recent regulatory warnings from the FDA and CISA have highlighted the discovery of critical cybersecurity flaws in patient monitors from multiple manufacturers. The devices were found to contain hidden firmware backdoors, which could allow an unauthorised attacker to gain remote access and potentially manipulate patient data. While no patient harm has been reported, the discovery has sent a clear signal to the industry that medical devices must be secure-by-design. This has led to a shift in procurement, with nearly half of healthcare buyers now declining device purchases over cybersecurity concerns.

The integrity of data from medical devices is paramount for patient safety. A compromised device could lead to misdiagnosis, incorrect treatment, or a delay in care. For medical device manufacturers, this is a wake-up call that cybersecurity is now a non-negotiable requirement for market access.

Recommendations:

- Medical device manufacturers should conduct thorough security testing, including penetration testing, to identify and eliminate backdoors and other vulnerabilities before going to market.
- Healthcare providers should demand a Software Bill of Materials (SBOM) and evidence of secure design practices from device manufacturers during procurement.
- Isolate medical devices on segmented networks to limit their exposure to potential threats.
- Monitor network traffic to and from medical devices for any suspicious activity.