Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 March 2026

Vulnerabilities

Critical n8n Flaws Allow Remote Code Execution and Exposure of Stored Credentials

The Hacker News - 11 March 2026 21:21

Cybersecurity researchers have disclosed details of two now-patched security flaws in the n8n workflow automation platform, including two critical bugs that could result in arbitrary command execution.

The vulnerabilities are listed below

-CVE-2026-27577 (CVSS score: 9.4) - Expression sandbox escape leading to remote code execution (RCE)

-CVE-2026-27493 (CVSS score: 9.5) – Unauthenticated expression evaluation via n8n's Form nodes

SQLi flaw in Elementor Ally plugin impacts 250k+ WordPress sites

BleepingComputer - 11 March 2026 16:38

An SQL injection vulnerability in Ally, a WordPress plugin from Elementor for web accessibility and usability with more than 400,000 installations, could be exploited to steal sensitive data without authentication.

Dozens of Vendors Patch Security Flaws Across Enterprise Software and Network Devices

The Hacker News - 11 March 2026 18:56

SAP has released security updates to address two critical security flaws that could be exploited to achieve arbitrary code execution on affected systems.

Microsoft Patches 84 Flaws in March Patch Tuesday, Including Two Public Zero-Days

The Hacker News - 11 March 2026 15:45

Microsoft on Tuesday released patches for a set of 84 new security vulnerabilities affecting various software components, including two that have been listed as publicly known. Of these, eight are rated Critical, and 76 are rated Important in severity.

Scottish Cyber Coordination Centre

Threat actors and malware

New PhantomRaven NPM attack wave steals dev data via 88 packages

BleepingComputer - 11 March 2026 14:09

New attack waves from the 'PhantomRaven' supply-chain campaign are hitting the npm registry, with dozens of malicious packages that exfiltrate sensitive data from JavaScript developers.

China's CERT warns OpenClaw can inflict nasty wounds

The Register - 12 March 2026 02:37

Like deleting data, exposing keys, and loading malicious content - which may be why Beijing has reportedly banned it China's National Computer Network Emergency Response Technical Team has warned locals that the OpenClaw agentic AI tool poses significant security risks.

UK incidents

Cyber-Attacks on UK Firms Increase at Four Times Global Rate

Infosecurity Magazine - 11 March 2026 11:30

Check Point data shows attack volumes are growing much faster in the UK than worldwide.