Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 February 2026

Vulnerabilities

Fresh SolarWinds Vulnerability Exploited in Attacks

SecurityWeek - 04 February 2026 10:50

The critical-severity SolarWinds Web Help Desk flaw could lead to unauthenticated remote code execution.

Critical n8n flaws disclosed along with public exploits

BleepingComputer - 04 February 2026 17:14

Multiple critical vulnerabilities in the popular n8n open-source workflow automation platform allow escaping the confines of the environment and taking complete control of the host server.

CVE-2025-22225 in VMware ESXi now used in active ransomware attacks

Security Affairs - 04 February 2026 23:02

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) confirms that ransomware gangs are exploiting the VMware ESXi sandbox escape flaw CVE-2025-22225. The vulnerability is an arbitrary write issue in VMware ESXi.

Google Looker Bugs Allow Cross-Tenant RCE, Data Exfil

darkreading - 04 February 2026 12:00

Attackers could even have used one vulnerable Lookout user to gain access to other GCP tenants' environments.

Threat actors and malware

Hackers compromise NGINX servers to redirect user traffic

BleepingComputer - 04 February 2026 19:26

A threat actor is compromising NGINX servers in a campaign that hijacks user traffic and reroutes it through the attacker's backend infrastructure.

Microsoft: Info-Stealing malware expands from Windows to macOS

Security Affairs - 04 February 2026 12:30

Microsoft warns info-stealing attacks are expanding from Windows to macOS, using cross-platform languages like Python and abusing trusted platforms.

Scottish Cyber Coordination Centre

DEAD#VAX Malware Campaign Deploys AsyncRAT via IPFS-Hosted VHD Phishing Files

The Hacker News - 04 February 2026 23:54

Threat hunters have disclosed details of a new, stealthy malware campaign dubbed DEAD#VAX that employs a mix of “disciplined tradecraft and clever abuse of legitimate system features” to bypass traditional detection mechanisms and deploy a remote access trojan (RAT) known as AsyncRAT.

China-Linked Amaranth-Dragon Exploits WinRAR Flaw in Espionage Campaigns

The Hacker News - 04 February 2026 20:39

Check Point Research is tracking the previously undocumented activity cluster under the moniker Amaranth-Dragon, which it said shares links to the APT 41 ecosystem.

Ransomware Gang Goes Full ‘Godfather’ With Cartel

darkreading - 04 February 2026 23:14

Since its launch in 2023, DragonForce has pushed a cartel model, emphasizing cooperation and coordination among ransomware gangs.