Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

25 February 2026

Vulnerabilities

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2026-25108 Soliton Systems K.K. FileZen OS Command Injection Vulnerability

SolarWinds patches four critical Serv-U flaws enabling root access

Security Affairs - 24 February 2026 21:07

SolarWinds released updates fixing four critical Serv-U vulnerabilities that allow remote code execution, potentially giving attackers full root access on unpatched servers. Serv-U is a file transfer server software that allows organizations to securely transfer files over networks.

VMware Aria Operations flaws could enable remote attacks

Security Affairs - 24 February 2026 16:02

Broadcom has released security updates to address multiple vulnerabilities affecting VMware Aria Operations. VMware Aria Operations is an IT operations management platform that helps organizations monitor and optimize virtual, cloud, and hybrid environments.

RoguePilot Flaw in GitHub Codespaces Enabled Copilot to Leak GITHUB_TOKEN

The Hacker News - 25 February 2026 01:22

A vulnerability in GitHub Codespaces could have been exploited by bad actors to seize control of repositories by injecting malicious Copilot instructions in a GitHub issue. The artificial intelligence (AI)-driven vulnerability has been codenamed RoguePilot by Orca Security. It has since been patched by Microsoft following responsible disclosure.

Threat actors and malware

Lazarus Group Picks a New Poison: Medusa Ransomware

darkreading - 24 February 2026 22:18

The North Korean threat group also leveraged Comebacker backdoor, Blindingcan RAT, and info stealer Infohook in its recent attacks.

New 'Sandworm_Mode' Supply Chain Attack Hits NPM

SecurityWeek - 24 February 2026 14:40

The malicious code propagates like a worm, poisons AI assistants, exfiltrates secrets, and contains a destructive dead switch.

Phishing campaign targets freight and logistics orgs in the US, Europe

BleepingComputer - 24 February 2026 19:57

A financially motivated threat group dubbed "Diesel Vortex" is stealing credentials from freight and logistics operators in the U.S. and Europe in phishing attacks using 52 domains.

'Arkanix Stealer' Malware Disappears Shortly After Debut

SecurityWeek - 24 February 2026 16:20

Written in C++ and Python, the malware exfiltrates system information, browser data, and steals files.

UK incidents

UK data watchdog fines Reddit £14.47M for letting kids slip past the gate

The Register - 24 February 2026 14:29

The UK's data protection regulator has fined social media giant Reddit £14.47 million ($19.5 million) over its use of children's data.