Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

26 February 2026

Vulnerabilities

CISA and Partners Release Guidance for Ongoing Global Exploitation of Cisco SD-WAN Systems

CISA Advisories -

The purpose of this Alert is to provide resources for organizations with Cisco Software-Defined Wide-Area Networking (SD-WAN) systems. CISA has added CVE-2026-20127 and CVE-2022-20775 to its Known Exploited Vulnerabilities (KEV) Catalog on Feb. 25, 2026.

Zyxel warns of critical RCE flaw affecting over a dozen routers

BleepingComputer - 25 February 2026 08:53

Taiwan networking provider Zyxel has released security updates to address a critical vulnerability affecting over a dozen router models that can allow unauthenticated attackers to gain remote command execution on unpatched devices.

SolarWinds Patches 4 Critical Serv-U 15.5 Flaws Allowing Root Code Execution

The Hacker News - 25 February 2026 13:34

SolarWinds has released updates to address four critical security flaws in its Serv-U file transfer software that, if successfully exploited, could result in remote code execution, the vulnerabilities, all rated 9.1 on the CVSS scoring system.

Flaws in Claude Code Put Developers' Machines at Risk

darkreading - 25 February 2026 23:02

The vulnerabilities highlight a big drawback to integrating AI into software development workflows and the potential impact on supply chains.

Threat actors and malware

Google Disrupts UNC2814 GRIDTIDE Campaign After 53 Breaches Across 42 Countries

The Hacker News - 26 February 2026 00:16

Google on Wednesday disclosed that it worked with industry partners to disrupt the infrastructure of a suspected China-nexus cyber espionage group tracked as UNC2814 that breached at least 53 organizations across 42 countries.

RAMP Forum Seizure Fractures Ransomware Ecosystem

darkreading - 25 February 2026 22:14

Researchers suggest defenders monitor how these malicious groups re-form and leverage the useful threat intel to guide their next moves.

Emulating the Mutative BlackByte Ransomware

Security Boulevard - 25 February 2026 19:17

AttackIQ has released a new attack graph that emulates the behaviors exhibited by BlackByte ransomware, a strain operated under the Ransomware-as-a-Service (RaaS) model that emerged in July 2021. Since its emergence, BlackByte has targeted organizations worldwide, including entities within U.S. critical infrastructure sectors such as Government, Financial Services, Manufacturing, and Energy.