Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 January 2026

Vulnerabilities

Fortinet Releases Guidance to Address Ongoing Exploitation of Authentication Bypass Vulnerability CVE-2026-24858

CISA Advisories -

Newly disclosed vulnerability Common Vulnerabilities and Exposures (CVE)-2026-24858 [Common Weakness Enumeration

Google Warns of Active Exploitation of WinRAR Vulnerability CVE-2025-8088

The Hacker News - 28 January 2026 16:16

Google on Tuesday revealed that multiple threat actors, including nation-state adversaries and financially motivated groups, are exploiting a now-patched critical security flaw in RARLAB WinRAR to establish initial access and deploy a diverse array of payloads.

SolarWinds warns of critical Web Help Desk RCE, auth bypass flaws

BleepingComputer - 28 January 2026 10:39

SolarWinds has released security updates to patch critical authentication bypass and remote command execution vulnerabilities in its Web Help Desk IT help desk software.

New sandbox escape flaw exposes n8n instances to RCE attacks

BleepingComputer - 28 January 2026 13:46

Two vulnerabilities in the n8n workflow automation platform could allow attackers to fully compromise affected instances, access sensitive data, and execute arbitrary code on the underlying host.

Threat actors and malware

Mustang Panda Deploys Updated COOLCLIENT Backdoor in Government Cyber Attacks

The Hacker News - 28 January 2026 18:10

Threat actors with ties to China have been observed using an updated version of a backdoor called COOLCLIENT in cyber espionage attacks in 2025 to facilitate comprehensive data theft from infected endpoints.

Scottish Cyber Coordination Centre

Initial access hackers switch to Tsundere Bot for ransomware attacks

BleepingComputer - 28 January 2026 19:29

A prolific initial access broker tracked as TA584 has been observed using the Tsundere Bot alongside XWorm remote access trojan to gain network access that could lead to ransomware attacks.

FBI seizes RAMP cybercrime forum used by ransomware gangs

BleepingComputer - 28 January 2026 13:38

The FBI has seized the notorious RAMP cybercrime forum, a platform used to advertise a wide range of malware and hacking services, and one of the few remaining forums that openly allowed the promotion of ransomware operations.