Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 August 2025

Vulnerabilities

Exploit weaponizes SAP NetWeaver bugs for full system compromise

Security Affairs - 20 August 2025 01:01

A new exploit chaining two vulnerabilities, tracked as CVE-2025-31324 and CVE-2025-42999, in SAP NetWeaver exposes organizations to the risk of system compromise and data theft.

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-2025-54948 Trend Micro Apex One OS Command Injection Vulnerability

Elastic rejects claims of a zero-day RCE flaw in Defend EDR

BleepingComputer - 19 August 2025 13:41

Enterprise search and security company Elastic is rejecting reports of a zero-day vulnerability impacting its Defend endpoint detection and response (EDR) product.

Attacker “Patches” Vulnerability Post Exploitation to Lock Out Competition

Infosecurity Magazine - 19 August 2025 14:00

Red Canary observed the novel tactic in a cluster of activity targeting a legacy vulnerability to access cloud-based Linux systems.

Threat actors and malware

Okta open-sources catalog of Auth0 rules for threat detection

BleepingComputer - 19 August 2025 15:17

Okta has open-sourced ready-made Sigma-based queries for Auth0 customers to detect account takeovers, misconfigurations, and suspicious behavior in event logs.

PipeMagic Backdoor Resurfaces as Part of Play Ransomware Attack Chain

darkreading - 19 August 2025 18:16

Attackers are wielding the sophisticated modular malware while exploiting CVE-2025-29824, a previously zero-day flaw in Windows Common Log File System (CLFS) that allows attackers to gain system-level privileges on compromised systems.

Scottish Cyber Coordination Centre

New GodRAT Trojan Targets Trading Firms Using Steganography and Gh0st RAT Code

The Hacker News - 19 August 2025 21:03

Financial institutions like trading and brokerage firms are the target of a new campaign that delivers a previously unreported remote access trojan called GodRAT. The malicious activity involves the “distribution of malicious .SCR (screen saver) files disguised as financial documents via Skype messenger.