Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 April 2025

Vulnerabilities

Critical Apache Roller Vulnerability (CVSS 10.0) Enables Unauthorized Session Persistence

The Hacker News - 15 April 2025 20:14

A critical security vulnerability has been disclosed in the Apache Roller open-source, Java-based blogging server software that could allow malicious actors to retain unauthorized access even after a password change. The flaw, assigned the CVE identifier CVE-2025-24859, carries a CVSS score of 10.0, indicating maximum severity.

Gladinet flaw CVE-2025-30406 actively exploited in the wild

Security Affairs - 15 April 2025 08:05

Security researchers at Huntress warn of attacks in the wild exploiting a critical vulnerability, tracked as CVE-2025-30406, in Gladinet CentreStack and Triofox software. The vulnerability CVE-2025-30406 (CVSS score 9.0) is a deserialization issue due to the CentreStack portal's hardcoded machineKey use.

Threat actors and malware

Midnight Blizzard deploys new GrapeLoader malware in embassy phishing

BleepingComputer - 15 April 2025 17:25

Russian state-sponsored espionage group Midnight Blizzard is behind a new spear-phishing campaign targeting diplomatic entities in Europe, including embassies.

Chinese Hackers Target Linux Systems Using SNOWLIGHT Malware and VShell Tool

The Hacker News - 15 April 2025 20:36

The China-linked threat actor known as UNC5174 has been attributed to a new campaign that leverages a variant of a known malware dubbed SNOWLIGHT and a new open-source tool called VShell to infect Linux systems.

Hertz disclosed a data breach following 2024 Cleo zero-day attack

Security Affairs - 15 April 2025 09:23

Hertz Corporation disclosed a data breach after customer data was stolen via Cleo zero-day exploits in late 2024, affecting Hertz, Thrifty, and Dollar brands.