



Daily Threat Bulletin

24 December 2025

Vulnerabilities

[WebRAT malware spread via fake vulnerability exploits on GitHub](#)

BleepingComputer - 23 December 2025 15:31

The WebRAT malware is now being distributed through GitHub repositories that claim to host proof-of-concept exploits for recently disclosed vulnerabilities.

[Critical n8n Flaw \(CVSS 9.9\) Enables Arbitrary Code Execution Across Thousands of Instances](#)

The Hacker News - 23 December 2025 14:04

A critical security vulnerability has been disclosed in the n8n workflow automation platform that, if successfully exploited, could result in arbitrary code execution under certain circumstances. The vulnerability, tracked as CVE-2025-68613, carries a CVSS score of 9.9.

Threat actors and malware

[Cyberattack knocks offline France's postal, banking services](#)

BleepingComputer - 23 December 2025 08:26

The French national postal service's online services were knocked offline by "a major network incident" on Monday, disrupting digital banking and other services for millions.

[Clop Ransomware Group Linked to 3.5m University of Phoenix Breach](#)

Infosecurity Magazine - 23 December 2025 17:00

A University of Phoenix data breach affecting nearly 3.5 million individuals has been claimed by the Clop ransomware collective.

[Denmark Accuses Russia of Conducting Two Cyberattacks](#)

Schneier on Security - 23 December 2025 13:02

The Danish Defence Intelligence Service (DDIS) announced on Thursday that Moscow was behind a cyber-attack on a Danish water utility in 2024 and a series of distributed denial-of-service (DDoS) attacks on Danish websites in the lead-up to the municipal and regional council elections in November.



Scottish
Cyber
Coordination
Centre

UK related

574 Arrested, \$3 Million Seized in Crackdown on African Cybercrime Rings

SecurityWeek - 23 December 2025 10:31

Authorities in Senegal, Ghana, Benin, and Cameroon dismantled BEC, ransomware, and other cyber-fraud networks.