Scottish Cyber Coordination Centre

Daily Threat Bulletin

1 December 2025

Vulnerabilities

CISA Adds Actively Exploited XSS Bug CVE-2021-26829 in OpenPLC ScadaBR to KEV

The Hacker News - 30 November 2025 15:53

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has updated its Known Exploited Vulnerabilities (KEV) catalog to include a security flaw impacting OpenPLC ScadaBR, citing evidence of active exploitation.

How CVSS v4.0 works: characterizing and scoring vulnerabilities

Malwarebytes - 28 November 2025 13:42

This blog explains why vulnerability scoring matters, how CVSS works, and what's new in version 4.0.

Threat actors and malware

Contagious Interview campaign expands with 197 npm Ppackages spreading new OtterCookie malware

Security Affairs - 30 November 2025 02:02

North Korea-linked actors behind Contagious Interview uploaded 197 new malicious npm packages to distribute a new OtterCookie malware version.

Tomiris Shifts to Public-Service Implants for Stealthier C2 in Attacks on Government Targets

The Hacker News - 01 December 2025 11:37

The threat actor known as Tomiris has been attributed to attacks targeting foreign ministries, intergovernmental organizations, and government entities in Russia with an aim to establish remote access and deploy additional tools.

Threat Actors Exploit Calendar Subscriptions for Phishing and Malware Delivery

Infosecurity Magazine - 28 November 2025 16:05

BitSight research has revealed how threat actors exploit calendar subscriptions to deliver phishing links, malware and social engineering attacks through hijacked domains.

Scottish Cyber Coordination Centre

UK incidents

Brit telco Brsk confirms breach as bidding begins for 230K+ customer records

The Register - 28 November 2025 16:52

British telco Brsk is investigating claims that it was attacked by cybercriminals who made off with more than 230,000 files.