



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

23 December 2025

Vulnerabilities

[Weekly Recap: Firewall Exploits, AI Data Theft, Android Hacks & More](#)

The Hacker News - 22 December 2025 18:30

Cyber threats last week showed how attackers no longer need big hacks to cause big damage. They're going after the everyday tools we trust most — firewalls, browser add-ons, and even smart TVs.

[Threat Actors Exploit Zero-Day in WatchGuard Firebox Devices](#)

darkreading - 22 December 2025 21:29

With attacks on the critical firewall vulnerability, WatchGuard joins a list of edge device vendors that have been targeted in recent weeks.

Threat actors and malware

[Interpol-led action decrypts 6 ransomware strains, arrests hundreds](#)

BleepingComputer - 22 December 2025 14:38

An Interpol-coordinated initiative called Operation Sentinel led to the arrest of 574 individuals and the recovery of \$3 million linked to business email compromise, extortion, and ransomware incidents.

[Romanian Waters confirms cyberattack, critical water operations unaffected](#)

Security Affairs - 22 December 2025 21:41

Romania's national water management authority, Romanian Waters, was hit by a ransomware attack.

[CISA and Partners Release Update to Malware Analysis Report BRICKSTORM Backdoor](#)

CISA Advisories -

Today, the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, and Canadian Centre for Cyber Security released an update to the Malware Analysis Report BRICKSTORM Backdoor with indicators of compromise (IOCs) and detection signatures for additional BRICKSTORM samples.



Scottish
Cyber
Coordination
Centre

UK related

[UK Government Acknowledges It Is Investigating Cyber Incident After Media Reports](#)

SecurityWeek - 22 December 2025 10:01

The British government is investigating a “cyber incident” following news reports that hackers linked to China have gained access to thousands of confidential documents.