



Scottish  
Cyber  
Coordination  
Centre

# Daily Threat Bulletin

22 December 2025

## Vulnerabilities

### [CISA Adds Three Known Exploited Vulnerabilities to Catalog](#)

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2025-20393 Cisco Multiple Products Improper Input Validation Vulnerability

CVE-2025-40602 SonicWall SMA1000 Missing Authorization Vulnerability

CVE-2025-59374 ASUS Live Update Embedded Malicious Code Vulnerability.

## Threat actors and malware

### [Android Malware Operations Merge Droppers, SMS Theft, and RAT Capabilities at Scale](#)

The Hacker News - 22 December 2025 12:41

Threat actors have been observed leveraging malicious dropper apps masquerading as legitimate applications to deliver an Android SMS stealer dubbed Wonderland in mobile attacks.

### [Iranian Infy APT Resurfaces with New Malware Activity After Years of Silence](#)

The Hacker News - 21 December 2025 10:52

Threat hunters have discerned new activity associated with an Iranian threat actor known as Infy (aka Prince of Persia), nearly five years after the hacking group was observed targeting victims in Sweden, the Netherlands, and Turkey.

### [There's so much stolen data in the world, South Korea will require face scans to buy a SIM](#)

The Register - 22 December 2025 05:11

South Korea's government on Friday announced it will require local mobile carriers to verify the identity of new customers with facial recognition scans, in the hope of reducing scams.



Scottish  
Cyber  
Coordination  
Centre

## UK related

### Cybersecurity Performance Goals 2.0 for Critical Infrastructure

CISA Advisories -

Today, CISA released updated Cross-Sector Cybersecurity Performance Goals (CPG 2.0) with measurable actions for critical infrastructure owners and operators to achieve a foundational level of cybersecurity.