Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 April 2026

Vulnerabilities

CISA flags new SD-WAN flaw as actively exploited in attacks

BleepingComputer - 21 April 2026 09:30

CISA has given U.S. government agencies four days to secure their systems against another Catalyst SD-WAN Manager vulnerability it flagged as actively exploited in attacks.

Actively exploited Apache ActiveMQ flaw impacts 6,400 servers

BleepingComputer - 21 April 2026 08:17

Nonprofit security organization Shadowserver found that over 6,400 Apache ActiveMQ servers exposed online are vulnerable to ongoing attacks exploiting a high-severity code injection vulnerability.

CISA Adds 8 Exploited Flaws to KEV, Sets April-May 2026 Federal Deadlines

The Hacker News - 21 April 2026 12:53

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added eight new vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog, including three flaws impacting Cisco Catalyst SD-WAN Manager, citing evidence of active exploitation.

Threat actors and malware

NGate Android malware uses HandyPay NFC app to steal card data

BleepingComputer - 21 April 2026 06:00

A new variant of the NGate malware that steals NFC payment data is targeting Android users by hiding in a trojanized version of HandyPay, a legitimate mobile payments processing tool.

SystemBC C2 Server Reveals 1,570+ Victims in The Gentlemen Ransomware Operation

The Hacker News - 22 April 2026 00:48

Threat actors associated with The Gentlemen ransomware-as-a-service (RaaS) operation have been observed attempting to deploy a known proxy malware called SystemBC. According to new research published by Check Point, the command-and-control (C2 or C&C) server linked to SystemBC has led to the discovery of a botnet of more than 1,570 victims.

Scottish Cyber Coordination Centre

macOS ClickFix attacks deliver AppleScript stealers to snarf credentials, wallets

The Register - 21 April 2026 16:50

Data from browsers, cryptocurrency wallets, 200+ extensions hoovered up A ClickFix campaign targeting macOS users delivers an AppleScript-based infostealer that collects credentials and live session cookies from 14 browsers, 16 cryptocurrency wallets, and more than 200 extensions.