Scottish Cyber Coordination Centre

Daily Threat Bulletin

13 April 2026

Vulnerabilities

Critical Marimo pre-auth RCE flaw now under active exploitation

BleepingComputer - 12 April 2026 11:20

A critical pre-authentication remote code execution (RCE) vulnerability in Marimo is now under active exploitation, leveraged for credential theft. [...]

Adobe fixes actively exploited Acrobat Reader flaw CVE-2026-34621

Security Affairs - 12 April 2026 18:47

Adobe addressed a critical Acrobat Reader vulnerability, tracked as CVE-2026-34621, which is actively exploited to run malicious code. Adobe released emergency updates to address a critical vulnerability, tracked as CVE-2026-34621 (CVSS score of 8.6), in Adobe Acrobat Reader, which is being actively exploited.

EngageLab SDK flaw opens door to private data on 50M Android devices

Security Affairs - 10 April 2026 09:41

A flaw in EngageLab SDK exposed up to 50M Android users, including 30M crypto wallets, letting apps bypass security and access private data. Microsoft researchers found a critical flaw in EngageSDK that lets apps bypass Android sandbox protections and access private data.

Juniper Networks Patches Dozens of Junos OS Vulnerabilities

SecurityWeek - 10 April 2026 14:44

A critical-severity flaw could be exploited remotely, without authentication, to take over a vulnerable device.

Orthanc DICOM Vulnerabilities Lead to Crashes, RCE

SecurityWeek - 10 April 2026 12:53

Attackers could exploit these vulnerabilities in denial-of-service, information disclosure, and arbitrary code execution attacks.

Chrome 147 Patches 60 Vulnerabilities, Including Two Critical Flaws Worth $86,000

SecurityWeek - 10 April 2026 11:44

The critical vulnerabilities affect Chrome's WebML component and they have been reported by anonymous researchers.

Scottish Cyber Coordination Centre

Threat actors and malware

Nearly 4,000 US industrial devices exposed to Iranian cyberattacks

BleepingComputer - 10 April 2026 12:52

The attack surface targeted by Iranian-linked hackers in cyberattacks against U.S. critical infrastructure networks includes thousands of Internet-exposed programmable logic controllers (PLCs) manufactured by Rockwell Automation. [...]

CPUID hacked to deliver malware via CPU-Z, HWMonitor downloads

BleepingComputer - 10 April 2026 10:12

Hackers gained access to an API for the CPUID project and changed the download links on the official website to serve malicious executables for the popular CPU-Z and HWMonitor tools. [...]

GlassWorm Campaign Uses Zig Dropper to Infect Multiple Developer IDEs

The Hacker News - 10 April 2026 19:53

Cybersecurity researchers have flagged yet another evolution of the ongoing GlassWorm campaign, which employs a new Zig dropper that's designed to stealthily infect all integrated development environments (IDEs) on a developer's machine.

Fake Claude site installs malware that gives attackers access to your computer

Malwarebytes - 10 April 2026 17:16

We found a convincing fake site that installs a trojanized Claude app while quietly deploying PlugX malware.