Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 July 2026

Vulnerabilities

CC-4808 - Active Exploitation of CVE-2026-48282 in Adobe ColdFusion

NHS Digital - 03 July 2026 10:21

Severity: Medium Successful exploitation could lead to arbitrary code execution in the context of the current user Successful exploitation could lead to arbitrary code execution in the context of the current user Updated: 03 Jul 2026

Unpatched Flaws Disclosed in Filesystem Bundled Into Millions of Embedded Devices

The Hacker News - 04 July 2026 02:49

Security firm runZero has disclosed seven vulnerabilities in FatFs, a small filesystem library that lets a device read and write the FAT and exFAT formats used on USB drives and SD cards.The flaws matter because FatFs is nearly everywhere. It ships inside the firmware that runs security cameras, drones, industrial controllers, hardware crypto wallets, and other devices built on

New “Bad Epoll” Linux Kernel Flaw Lets Unprivileged Users Gain Root, Hits Android

The Hacker News - 04 July 2026 02:10

A newly disclosed Linux kernel flaw called Bad Epoll (CVE-2026-46242) lets an ordinary user with no special access take full control of a machine as root. It affects Linux desktops, servers, and Android, and a fix is out.Bad Epoll sits in the same small stretch of kernel code where Anthropic’s most powerful AI model, Mythos, recently found a different bug.The AI caught one flaw and missed

Critical Cursor AI Code Editor Flaws Could Lead to OS-Level Remote Code Execution

SecurityWeek - 03 July 2026 08:57

The DuneSlide vulnerabilities enable zero-click prompt injection attacks that escape Cursor’s sandbox and execute arbitrary code on the underlying operating system.The post Critical Cursor AI Code Editor Flaws Could Lead to OS-Level Remote Code Execution appeared first on SecurityWeek.

XZ Utils vulnerability impacting B&R Products

CISA Advisories -

An update is available that resolves vulnerability in the product versions listed as affected in the advisory. An attacker who successfully exploited this vulnerability could cause the product to stop or corrupt memory data. The following versions of XZ Utils vulnerability impacting B&R Products are affected:PPC3100 <1.8.1, 1.8.1 (CVE-2025-31115)C50 <1.8.0, 1.8.0 (CVE-2025-31115)C80

<1.8.0, 1.8.0 (CVE-2025-31115)FT50 <1.8.1, 1.8.1 (CVE-2025-31115)MT50 <1.8.1, 1.8.1 (CVE-2025-31115)T30 <1.8.0, 1.8.0 (CVE-2025-31115)T80 <1.8.0, 1.8.0 (CVE-2025-31115)T50 <1.8.1, 1.8.1 (CVE-2025-31115)

Threat actors and malware

JadePuffer ransomware used AI agent to automate entire attack

BleepingComputer - 04 July 2026 11:16

Researchers identified what they believe is the first documented case of a ransomware operation, JadePuffer, conducted entirely by a large language model (LLM) agent. [...]

New Avalon Malware Framework Packs CrownX Ransomware Capabilities

The Hacker News - 04 July 2026 01:25

Cybersecurity researchers have discovered a previously undocumented modular malware framework codenamed Avalon that's distributed by means of a multi-stage phishing chain capable of bypassing traditional security controls.

Chinese LLMs Broaden the Gap Between Attackers & Defenders

darkreading - 03 July 2026 14:01

Two new models from Chinese firms compete with top US mainstream and frontier models. Should cyber-defenders be worried?

UK related

PCI DSS explained for small merchants: a practical guide for UK SMEs

Security Boulevard - 05 July 2026 14:59

PCI DSS explained for small merchants: a practical guide for UK SMEs If your business takes card payments, PCI DSS is worth understanding. It can feel like another layer of compliance work, but for most small merchants the real issue is simpler: how to protect customer card data, reduce the chance of a payment-related incident, [...]