Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 August 2026

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-2023-49105 ownCloud Improper Authentication Vulnerability

CVE-2026-53362 Linux Kernel Unspecified Vulnerability

CVE-2026-66384 JFrog Artifactory Improper Limitation of a Pathname to a Restricted Directory Vulnerability

PaperCut warns of NG, MF flaw exploited in zero-day attacks

BleepingComputer - 27 August 2026 13:31

PaperCut is warning that hackers are actively exploiting a vulnerability in all versions of its PaperCut NG and PaperCut MF print management software in zero-day attacks.

Next.js Patches Critical AVIF and Windows Flaws Enabling Unauthenticated RCE

The Hacker News - 27 August 2026 21:43

Credit: HacktronVercel has released security patches for two critical-severity vulnerabilities in the Next.js web framework, both of which allow unauthenticated remote code execution, one exploitable via specially crafted AVIF image files and the other through a path traversal flaw affecting servers that use a Windows filesystem.

Threat actors and malware

Nearly 700 rogue AI agents coordinated in the Hugging Face attack

BleepingComputer - 27 August 2026 18:38

New details about the July attack on Hugging Face reveal that hundreds of AI agents driven by OpenAI's internal IM1 model coordinated the compromise through an unauthorized message board.

Dark Caracal Deploys New Go Malware With Ethereum-Based C2 Fallback

Security Affairs - 27 August 2026 21:31

Dark Caracal targets Venezuela with GoCaracal, an upgraded Bandook toolkit and an Ethereum fallback for resilient C2 communications. Dark Caracal is back with new malware and the same hunting grounds.

Scottish Cyber Coordination Centre

Chinese Routers Sold Worldwide Contain Backdoors

darkreading - 27 August 2026 20:31

An untold number of ZBT routers sold around the world as white-label products come with several implants built by the manufacturer.

Cyberattack Causes Global Disruption at Boston Scientific

SecurityWeek - 27 August 2026 11:18

The cybersecurity incident has disrupted Boston Scientific's ability to process and ship customer orders.

UK incidents

Manchester Airports Group says hackers stole travelers' data

BleepingComputer - 27 August 2026 13:12

The Manchester Airports Group (MAG) disclosed that hackers breached its systems and stole customer data, including Wi-Fi sign-ups from Manchester, Stansted, and East Midlands airports.