Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 August 2026

Vulnerabilities

Rails patches critical Active Storage flaw with RCE potential

Bleeping Computer - 01 August 2026 10:20

A critical vulnerability in the Active Storage framework can allow an unauthenticated attacker to read arbitrary files from a Rails application, and potentially escalate to remote code execution (RCE). [...]

Adobe fixed a maximum-severity vulnerability flaw in Campaign Classic

Security Affairs - 01 August 2026 12:31

Adobe fixed a maximum severity vulnerability in Campaign Classic that could let attackers run code remotely without user interaction. Adobe has addressed a critical vulnerability, tracked as CVE-2026-48449 (CVSS score of 10.0), in Adobe Campaign Classic, the company's enterprise marketing automation platform.

Google AI Supercharges Chrome Security, Fixing 1,072 Bugs

Security Affairs - 31 July 2026 13:46

Google says AI found and helped fix 1,072 Chrome security bugs in two releases, dramatically accelerating vulnerability detection and patching Google's Chrome Security team published a detailed account of how AI models have transformed their vulnerability management pipeline, and the headline figure is difficult to dismiss: in the last two Chrome releases alone, the team [...]

Three Recent Chrome Releases Fix 1,442 Flaws, More Than Prior 23 Updates Combined

The Hacker News - 31 July 2026 18:21

Google on Thursday announced that it fixed a whopping 1,072 security bugs in Chrome versions 149 and 150, surpassing the total number of flaws the company fixed across the prior 23 milestones combined.

Researchers Report 84 Flaws in 4G and 5G Cores, Including a Session Hijacking Flaw

The Hacker News - 31 July 2026 17:25

An academic study has disclosed a "widespread class" of security vulnerabilities impacting 4G and 5G core networks that, if successfully exploited, could trigger denial-of-service (DoS) attacks and even session hijacking, allowing an attacker to seize control of a user's network session.

Scottish Cyber Coordination Centre

Critical Flaw Allowed to Azure Cosmos DB Pwnage

Security Week - 31 July 2026 09:04

Named CosmosEscape, the vulnerability exposed the primary key for Cosmos DB accounts, granting full read and write access.

Critical Code Execution Vulnerability Patched in TeamCity

Security Week - 31 July 2026 06:50

Tracked as CVE-2026-63077, the security defect can be exploited without authentication via the agent polling protocol.

Threat actors and malware

Arch Linux disables AUR package adoption to stop malware flood

Bleeping Computer - 31 July 2026 17:38

The Arch Linux project has temporarily disabled adoption of Arch User Repository (AUR) packages after a surge in malicious takeovers of existing packages. [...]

Hacker uses DeepSeek AI to autonomously attack vulnerable servers

Bleeping Computer - 31 July 2026 13:35

A Chinese-speaking threat actor is using the DeepSeek AI model and the open-source Hermes Agent to conduct autonomous cyberattacks on exposed servers with limited human involvement. [...]

Russian Hackers Hijack Hotel Wi-Fi to Steal Microsoft 365 Tokens

Security Affairs - 01 August 2026 14:11

Microsoft says Russian hackers hijacked hotel Wi-Fi portals to spread malware and steal Microsoft 365 tokens from travelers. Microsoft Threat Intelligence disclosed CaptiveCrunch, a campaign it attributes to Storm-2945, an operational sub-cluster of Midnight Blizzard, the Russian SVR-linked group also known as APT29 and Cozy Bear.

Prompted by OpenAI Disclosure, Anthropic Finds Its Own Models Hacked 3 Organizations

Security Week - 31 July 2026 09:39

A security company's systems were hacked after it installed a malicious Python package deployed by Claude.