Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 August 2026

Vulnerabilities

U.S. CISA adds a JetBrains TeamCity flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 06 August 2026 09:22

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a JetBrains TeamCity vulnerability to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a JetBrains TeamCity vulnerability, tracked as CVE-2026-63077 (CVSS score of 9.8), to its Known Exploited Vulnerabilities (KEV) catalog. At the end of July,

New Zapscape KVM Flaw Could Let Privileged L1 Guest Code Escape to Linux Hosts

The Hacker News - 07 August 2026 00:28

Zapscape, a new Linux kernel vulnerability, could allow an attacker with kernel privileges inside an L1 guest virtual machine (VM) to escape KVM isolation and execute code on the host. The risk applies when nested virtualization is exposed to untrusted guests.

Cisco Patches 12 SD-WAN and IOS XE Flaws, Including Three 9.8 CVSS Score Bugs

The Hacker News - 06 August 2026 23:43

Cisco has rolled out updates to address multiple critical security vulnerabilities impacting Catalyst SD-WAN and IOS XE Software as part of a comprehensive internal security review.

AWS, Google, and Vercel Agent Flaws Let Attackers Trigger Tools Without Running the Model

The Hacker News - 06 August 2026 15:27

Security flaws in agent infrastructure from Amazon Web Services (AWS), Google, and Vercel let untrusted or forged instructions reach an agent's tools with no check that a model turn had authorized them.

Critical Vulnerabilities Patched With Chrome 151 Update

SecurityWeek - 07 August 2026 07:56

The browser refresh eliminates over two dozen memory safety bugs, including critical use-after-free flaws.

Critical Paperclip Flaw Allowed Admin Access, Code Execution

SecurityWeek - 06 August 2026 12:09

An attacker could self-register, sign in for board-level API access, and import a new company for code execution.

Threat actors and malware

Zbtlink Chinese Router Sold Worldwide Contains a Hidden Backdoor Affecting 20+ Models

Cyber Security News - 07 August 2026 07:38

Zbtlink routers sold in global markets have been found carrying a hidden remote-control implant that starts with the device. The discovery affects equipment used in homes, offices, temporary sites and vehicles, turning a trusted network gateway into a potential entry point. The affected devices may be present anywhere small, low-cost network hardware is deployed today. [...]

ClickFix attack pushes macOS infostealer for crypto theft attacks

BleepingComputer - 06 August 2026 19:37

A Go-based malware delivered in ClickFix attacks targeting macOS users is stealing cryptocurrency assets, browser-stored passwords, Apple Keychain data, and cached credentials. [...]

New TONTOU CPU attack bypasses Spectre v2 fixes, leaks Linux password hashes

BleepingComputer - 06 August 2026 15:03

Researchers found a way to bypass recent mitigations for Spectre v2 speculative execution side-channel attacks and developed an exploit to leak secrets from Linux machines. [...]

Meta AI model hacked a company during misconfigured cyber test

BleepingComputer - 06 August 2026 13:11

Meta has become the latest AI company to confirm that one of its models hacked a real organization during cybersecurity testing, as similar incidents continue to emerge following OpenAI'sOpenAI's initial disclosure that its agents breached Hugging Face. [...]

New Interrupt Injection Attack Can Bypass Spectre v2 Defenses on Intel and AMD CPUs

The Hacker News - 06 August 2026 22:47

An unprivileged Linux program can time a hardware interrupt to land in the gap between a processor sanitizing its branch predictor and the kernel using it, re-poisoning the predictor after the defense has run.MIT CSAIL researchers Daniël Trujillo and Mengjia Yan named the technique INTERRUPT INJECTION.

Attackers Compile khunt Inside Oracle to Turn SQL Injection Into Windows SYSTEM Access

The Hacker News - 06 August 2026 15:49

Scottish Cyber Coordination Centre

Attackers broke into an organization's Oracle database through a SQL injection flaw in a public-facing web application, then installed a post-exploitation toolkit without writing an executable to disk.

Anthropic's Mythos AI used social engineering to target real people

Malwarebytes - 06 August 2026 11:45

Testers found that Anthropic's AI agent Mythos attempted to social engineer Github developers into accepting malicious code.