Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 August 2026

Vulnerabilities

CC-4832 - Proof-of-Concept Exploit Released for Citrix NetScaler ADC and NetScaler Gateway Vulnerability

NHS Digital - 14 August 2026 12:06

Severity: Medium Security researchers have demonstrated that CVE-2026-8452 could lead to remote code execution (RCE) Security researchers have demonstrated that CVE-2026-8452 could lead to remote code execution (RCE) Updated: 14 Aug 2026

Max severity SAP Commerce Cloud flaw now targeted in attacks

Bleeping Computer - 14 August 2026 09:45

A maximum-severity SAP Commerce Cloud remote code execution vulnerability patched three days ago is already being targeted in attacks, according to threat intelligence company Defused. [...]

macOS Screen Sharing Flaw Exploited to Deploy Monero Miners

Security Affairs - 15 August 2026 08:34

Hackers are exploiting a macOS Screen Sharing flaw to gain root access and install Monero miners on Macs with port 5900 exposed online. The Dutch National Cyber Security Centre confirmed active exploitation of a critical macOS authentication flaw, tracked as CVE-2026-65400 (CVSS score of 9.8), less than two weeks after Apple shipped the fix. The [...]

GeoServer Zero-Day Is Already Being Probed. That's the Problem

Security Affairs - 15 August 2026 07:18

GeoServer faces an unpatched zero-day enabling SQL injection and potentially RCE, with attackers already probing exposed systems. A newly disclosed GeoServer zero-day is already attracting active exploitation attempts, and there is no patch available yet.

Chinese AI company Zhipu claims its new is a better bug-finder than Anthropic, OpenAI

The Register - 17 August 2026 02:51

PLUS: HCL, TCS, admit data breaches; Google, Apple, India bans some rideshare tips; and more!

Threat actors and malware

Large-scale DDoS attacks disrupted Threema secure messaging service

Scottish Cyber Coordination Centre

Bleeping Computer - 16 August 2026 13:29

Multiple distributed denial-of-service (DDoS) attacks targeted the Threema secure messaging service earlier this week, causing severe disruptions to communications. [...]

New Evooo1Bot Linux botnet turns routers into traffic relay nodes

Bleeping Computer - 15 August 2026 10:14

A new Mirai-based modular Linux botnet malware called Evooo1Bot has been targeting internet-facing gateway devices, turning them into SOCKS5 traffic relay nodes. [...]

APT36 Suspected in PATCHCORD Espionage Campaign Using Google Sheets C2

Security Affairs - 16 August 2026 07:24

Acronis uncovered PATCHCORD, a stealthy backdoor targeting Afghan telecom and South Asian infrastructure via fake VPN tools and Google Sheets C2. Researchers at Acronis just documented an espionage operation that reads like it was built by someone with genuinely good taste in disguises.

Novel macOS Infostealer AmnesiaStealer Spread via ClickFix

Infosecurity Magazine - 14 August 2026 10:45

AmnesiaStealer contains novel functions, including the attackers gaining remote control over the victim's browser to steal cookie data

Autonomous AI attacks pose 'clear and present danger' to critical infrastructure

The Register - 14 August 2026 15:03

Weaponized agents could turn digital intrusions into kinetic disasters, experts warn

Post-Hugging Face Reflections: The Agentic Attacker Is Already Here

Cyber Security News - 15 August 2026 14:34

Bill Robbins, CEO of Menlo Security An AI agent broke out of the sandbox built to contain it and put itself on the open internet. Then it attacked another company. The attack wasn't executed by a human. Instead, the AI agent independently selected and executed its next actions without a person issuing commands in real time. OpenAI disclosed that two of [...]