Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 August 2026

Vulnerabilities

TP-Link patches Omada ZTP flaws allowing hackers to breach networks

Bleeping Computer - 04 August 2026 18:18

TP-Link has patched 15 vulnerabilities in the zero-touch provisioning (ZTP) mechanism of its Omada network devices that could be chained with previously disclosed flaws to achieve remote code execution (RCE). [...]

SharePoint Flaws Used to Hack Switzerland's Federal IT Agency

Security Affairs - 04 August 2026 20:12

Swiss Federal IT Agency FOITT says attackers exploited SharePoint flaws to compromise about 200 accounts. Servers are being rebuilt as investigations continue. Switzerland's Federal Office for Information Technology and Communications, known as BIT or FOITT, disclosed that unknown attackers had compromised approximately 200 accounts on its on-premises SharePoint servers.

CVE-2026-58048: cPanel Bug Enables Full Database Administrator Access

Security Affairs - 04 August 2026 12:29

A critical cPanel flaw (CVE-2026-58048) lets authenticated users execute SQL as root. Users should update to fixed versions immediately. If you run a shared hosting box, this one's worth reading before your morning coffee gets cold. cPanel just patched a flaw, tracked as CVE-2026-58048 (CVSS score of 9.4), that let an ordinary authenticated hosting customer, [...]

U.S. CISA adds a N-able N-central flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 04 August 2026 11:02

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a N-able N-central flaw to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a N-able N-central flaw, tracked as CVE-2026-18577 (CVSS score of 8.2), to its Known Exploited Vulnerabilities (KEV) catalog. CVE-2026-18577 (CVSS 8.2) is an authentication bypass flaw caused by an [...]

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA - 04 August 2026 12:00

CISA has added three new vulnerabilities

Decades-Old BMC Vulnerability Exposes Thousands of Data Centers to Attacks

Security Week - 04 August 2026 09:56

Over 24,000 internet-accessible server-management interfaces disclose authentication hashes before login.The post

CISA Warns of Apache Tomcat Encryption Vulnerability Actively Exploited in Attacks

Cyber Security News - 05 August 2026 05:28

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a high-severity Apache Tomcat flaw, tracked as CVE-2026-34486, to its Known Exploited Vulnerabilities catalog.

Six Flowise RCE Flaws Let Attackers Execute Code on AI Workflow Servers

Cyber Security News - 04 August 2026 13:57

Flowise servers used to build AI agents and automated workflows are facing six newly disclosed remote code execution flaws. The weaknesses could allow authenticated attackers to run commands on the underlying server, putting data, credentials, and connected systems at risk.

Threat actors and malware

New XCSSET variant targets macOS devs via compromised Xcode projects

Bleeping Computer - 04 August 2026 15:03

A new version of the XCSSET malware is targeting thousands of macOS users through compromised Xcode projects and GitHub repositories. [...]

Massive ChainDrop npm supply-chain attack infects hundreds of packages

Bleeping Computer - 04 August 2026 11:24

Self-propagating malware named 'ChainDrop' has compromised more than 1,300 packages with a combined 2 billion monthly downloads on the Node Package Manager (npm) registry. [...]

INC Ransomware is Calling Victims – Pressure Tactics Post SonicWall Zero-Day Exploit

Security Affairs - 04 August 2026 13:46

INC Ransomware exploits SonicWall SMA 1000 flaws, using calls and emails to pressure victims during extortion campaigns targeting global organizations. Resecurity disclosed that INC Ransomware has emerged as the dominant threat actor exploiting the recently disclosed SonicWall Secure Mobile Access (SMA) 1000 vulnerabilities.

DOUBLECUP Uses ClickFix and Cached PNGs to Deliver CountLoader and DeviceManager RAT

The Hacker News - 04 August 2026 14:33

A new Russian loader-as-a-service (LaaS) codenamed DOUBLECUP has been using ClickFix lures as a way to stage malware-laced PNG images in victims' browser cache and ultimately deliver CountLoader and a previously undocumented remote access trojan called DeviceManager."The first stage drops a steganographic PNG image into the browser's cache, retrieves its hidden content, and executes the second

Hackers Can Weaponize Microsoft Copilot to Hijack CEO Accounts and Redirect Wire Transfers

Cyber Security News - 04 August 2026 17:07

A new proof-of-concept reveals how attackers can turn Microsoft Copilot, the AI assistant embedded in Microsoft 365, into an unwitting accomplice for business email compromise (BEC) and large-scale wire fraud. The demonstration shows that a single compromised employee account can escalate, with alarming speed, into full CEO account takeover and the theft of a quarter [...]

UK related

NCSC statement in response to recent incidents resulting from frontier AI evaluations

NCSC - 04 August 2026 12:00

A statement from Ollie Whitehouse, Chief Technology Officer at the NCSC, on AI security following recent incidents.

Mythos 5 and GPT-5.6-Sol Agents Went Beyond Their Cyber Test and Targeted the Real World

Cyber Security News - 05 August 2026 03:59

The UK's AI Security Institute (AISI) has disclosed a serious security incident in which AI agents under evaluation broke out of their intended test scope and took unsanctioned action against real people and organizations on the live internet. The incident, which unfolded between 25 and 28 July 2026, involved Anthropic's Mythos 5 and OpenAI's GPT-5.6-Sol, [...]