Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 August 2026

Vulnerabilities

CC-4827 - WordPress Releases Security Updates to Address “XSS2Shell” Vulnerability Chain

NHS Digital - 07 August 2026 14:53

Severity: Medium Successful exploitation of CVE-2026-64638 could potentially lead to PHP code execution Successful exploitation of CVE-2026-64638 could potentially lead to PHP code execution Updated: 07 Aug 2026

CC-4826 - JetBrains Releases Security Advisory for Critical Vulnerability CVE-2026-63077

NHS Digital - 07 August 2026 11:39

Severity: Medium Exploitation of CVE-2026-63077 could allow unauthenticated remote code execution on vulnerable TeamCity On-Premises servers Exploitation of CVE-2026-63077 could allow unauthenticated remote code execution on vulnerable TeamCity On-Premises servers Updated: 07 Aug 2026

Metabase Zero-Day Exploited in the Wild, Exposing Admin Access and Sensitive Data

Security Affairs - 08 August 2026 11:50

Attackers exploited a CVSS 10 Metabase zero-day to gain admin access and steal sensitive data. Framework confirmed it was among the victims. Metabase just confirmed something no analytics vendor wants to write: attackers found and used an unpatched, maximum-severity flaw against Metabase Cloud before anyone on the defense side knew it existed.

Progress Kemp LoadMaster Flaw Hits CISA KEV After 792 Reported Exploit Attempts

The Hacker News - 08 August 2026 12:22

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added a critical-severity security flaw impacting Progress Kemp LoadMaster to its Known Exploited Vulnerabilities (KEV) catalog, following reports of active exploitation in the wild.The vulnerability, tracked as CVE-2026-8037 (CVSS score: 9.6), is a command injection flaw that could be weaponized to achieve arbitrary

New WordPress Pre-Auth XSS Could Lead to PHP Code Execution - Patch ASAP

The Hacker News - 07 August 2026 18:26

WordPress has fixed a pre-authentication reflected cross-site scripting (XSS) flaw in its login screen that affects every version of the content management system. pwn.ai demonstrated how the flaw can be chained into PHP code execution on the server when a logged-in

administrator interacts with an attacker-controlled page.Tracked as CVE-2026-64638 (CVSS score: 8.9), the high-severity

AI-Generated Patches Fail Half the Time

Dark Reading - 07 August 2026 16:47

A study of more than 6,000 patches found that even working patches can introduce new bugs, break something else, or are open to bypass.

Critical One-Click Vulnerability in Atlassian's Rovo AI Exposed Enterprise Data

Security Week - 08 August 2026 11:30

The RovoBlast attack method identified by Varonis researchers could have been exploited to steal Confluence, Jira and SharePoint data.The post

Microsoft, Apple Release Fresh Security Updates

Security Week - 07 August 2026 09:09

Microsoft fixed critical vulnerabilities across Azure, Entra, and SharePoint, while Apple patched a high-severity authentication bypass.The post

Critical Vulnerabilities Patched With Chrome 151 Update

Security Week - 07 August 2026 06:56

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

N-able God mode flaw: Vendor confirms attackers reached customer networks as second hotfix lands

The Register - 07 August 2026 17:01

Attackers turned admin access into a route downstream, while N-able tells N-central customers to patch – again

Threat actors and malware

Hackers breach TrueConf to trojanize client installers with backdoors

Bleeping Computer - 08 August 2026 10:16

The Head Mare hacktivist group has been exploiting vulnerabilities in unpatched TrueConf video conferencing servers to replace client installers with malicious versions that deliver backdoors. [...]

Metabase SQLi zero-day exploited in customer data-theft attacks

Bleeping Computer - 07 August 2026 16:14

A critical Metabase SQL injection vulnerability was exploited in zero-day attacks to breach customer instances in data theft attacks, known to impact Framework and Tally. [...]

Scottish Cyber Coordination Centre

Palo Alto Networks Faces China Cybersecurity Review Amid Rising Tech Tensions

Security Affairs - 08 August 2026 13:41

China opened a cybersecurity review of Palo Alto Networks, citing national security concerns but giving no details about the reasons behind the probe. China's Cyberspace Administration (CAC) announced that it's launching a cybersecurity review of products Palo Alto Networks sells in the country. The announcement itself runs to a few sentences of formal Chinese, citing [...]

Hackers Impersonate IT Support to Breach Leading Financial Companies

Security Affairs - 07 August 2026 15:50

Hackers used fake IT help desks to steal MFA credentials, targeting over 200 firms, including major financial companies. A hacking campaign operating under names including Redact, Pink, Falcon, and Helix has built credential-stealing websites targeting employees at Blackstone, Bridgewater Associates, Apollo Global Management, Bain Capital, KKR, TPG, CME Group, Clearlake Capital, and Moody's, among dozens [...]

Atlassian Rovo Can Be Tricked Into Sending Jira and Confluence Data to Attackers

The Hacker News - 08 August 2026 14:24

Attacker-controlled instructions can make Atlassian's Rovo assistant collect Jira or Confluence data that a signed-in user can access, then send it to an outside server. Two security firms found that behavior independently, by different routes.

New CSS Attacks Can Break Webmail Defenses to Steal Passwords and Tokens

The Hacker News - 08 August 2026 13:33

New research shows content inside an email can escape its message boundary and interfere with the webmail interface.Across attack chains spanning Outlook, Gmail, Fastmail, Proton Mail, Yahoo Mail, and AOL Mail, the techniques can capture passwords, take over third-party accounts, leak tokens, hijack trusted UI actions, and manipulate AI tools that read email.PortSwigger researcher Gareth

N-able Issues N-central Hotfix 2 as Attackers Reach Managed Systems and Persist

The Hacker News - 08 August 2026 12:27

N-able has released a fresh round of hotfixes for N-central as part of its investigation into ongoing exploitation of a recently disclosed security flaw in the Remote Monitoring and Management (RMM) product."We are proactively expanding protections in response to ongoing monitoring of threat actors as they evolve their attack techniques," the company said."This is not a duplicate of our

Nearly 800 Malicious npm Packages Deliver Cross-Platform RAT and Infostealer

The Hacker News - 08 August 2026 00:18

A cluster of nearly 800 malicious packages has been published to the npm registry as part of a new campaign designed to deliver cross-platform malware targeting Windows, Mac, and

Linux systems."These packages appear to use AI slop squatted, or randomly generated typo-squatting package names, but all of them deliver a powerful RAT and infostealer payload," OpenSourceMalware researcher Paul

TeamPCP Linked To Redis Attacks Dating Back To 2020 And Later Supply Chain Campaign

The Hacker News - 07 August 2026 12:20

A new analysis has uncovered that the threat actor tracked as TeamPCP has been active on the cybercrime scene as far back as 2020, indicating the group has been compromising internet-facing infrastructure for years before training their sights on the software supply chain."The connection is supported by overlapping domains, malware deployment paths, staging techniques, backend infrastructure,

Ransomware attacks spike as world distracted by AI

The Register - 07 August 2026 18:45

What, you didn't think the top gangs were busy watching agents escape their sandboxes too, did you?