Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 September 2026

Vulnerabilities

Cisco confirms CVE-2026-20079 Secure FMC flaw exploited in attacks

BleepingComputer - 09 September 2026 18:40

Cisco has confirmed that a maximum-severity authentication bypass vulnerability tracked as CVE-2026-20079 in its Secure Firewall Management Center (FMC) software is being actively exploited in attacks.

Google fixes the seventh actively exploited Chrome zero-day of 2026

Security Affairs - 09 September 2026 14:47

Google patched 230 Chrome flaws, including an actively exploited V8 bug that could let attackers run arbitrary code through a crafted HTML page. Google released a Chrome update fixing 230 security vulnerabilities, including one already exploited in the wild tracked as CVE-2026-87491 (CVSS score of 8.8).

New cPanel Flaw Lets a Hosting Account With Mail Privileges Run Code as Root

The Hacker News - 09 September 2026 14:49

cPanel has patched a flaw that it says lets a single hosting account take control of an entire server. An authenticated account holder with mail-related privileges can create files of their choosing on the server through EmailTrack and, from there, run code as the root user.

Microsoft Patches Record 974 Flaws, Including Two Exploited Windows Zero-Days

The Hacker News - 09 September 2026 11:11

Microsoft on Tuesday broke Patch Tuesday records by addressing an earth-shattering 974 vulnerabilities spanning its software portfolio, including two flaws that it said have been actively exploited in the wild.These include 723 flaws in Windows, 111 in Office and Office 2016, 62 in SQL, and 22 in Developer Tools.

ICS Patch Tuesday: Schneider Electric, Siemens Fix Critical Flaws

SecurityWeek - 09 September 2026 11:49

AVEVA and Rockwell Automation also released patches for vulnerabilities affecting industrial control system products.The post ICS Patch Tuesday: Schneider Electric, Siemens Fix Critical Flaws appeared first on SecurityWeek.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-25249 Fortinet Multiple Products Heap-based Buffer Overflow Vulnerability; CVE-2026-19490 Citrix NetScaler Authentication Bypass Using an Alternate Path or Channel Vulnerability; CVE-2026-87491 Google Chromium V8 Out of Bounds Write Vulnerability; CVE-2026-20079 Cisco Firewall Management Center Authentication Bypass Using an Alternate Path or Channel Vulnerability.

Threat actors and malware

Cisco confirms CVE-2026-20079 Secure FMC flaw exploited in attacks

BleepingComputer - 09 September 2026 18:40

Cisco has confirmed that a maximum-severity authentication bypass vulnerability tracked as CVE-2026-20079 in its Secure Firewall Management Center (FMC) software is being actively exploited in attacks.

Four Nation-State Actors Used the Same Chrome Zero-Day Exploit Kit Within 12 Days

Security Affairs - 10 September 2026 06:35

Four espionage groups used the BlueMoon Chrome+Windows exploit kit within 12 days. Researchers suspect AI development. Proofpoint published a detailed analysis of a Chrome-and-Windows exploit kit it tracks as BlueMoon that four nation-state actors adopted within roughly two weeks of the first observed use.

F5 BIG-IP APM Malware Injects a PHP Web Shell Into Memory, Evading Disk Scans

The Hacker News - 09 September 2026 14:06

Malware linked to break-ins at F5 BIG-IP Access Policy Manager appliances hides a PHP web shell in memory instead of in a file on disk, Sophos said in an analysis published on September 7.

AI Is Giving Lesser-Resourced Attackers Nation-State-Level Reach, Google Warns

SecurityWeek - 09 September 2026 17:56

Criminal and state-sponsored adversaries are increasingly using AI to automate and scale their attacks, according to GTIG.The post AI Is Giving Lesser-Resourced Attackers Nation-State-Level Reach, Google Warns appeared first on SecurityWeek.

NHIs Now the Number One Corporate Entry Point for Hackers

Infosecurity Magazine - 09 September 2026 14:00

A new SpyCloud study claims that non-human identities (NHIs) including AI agents are nearly twice as likely to be a primary entry point into the enterprise than phishing.