Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 September 2026

Vulnerabilities

Critical Chrome 0-Day Vulnerability Actively Exploited in the Wild

Cyber Security News - 04 September 2026 07:17

Google has released an emergency Chrome security update that fixes a critical zero-day vulnerability already being exploited in real-world attacks.

OpenAI GPT-6 Astra Discovers Zero-Day Flaws and Builds Working Exploits in Cyber Tests

Cyber Security News - 04 September 2026 04:33

OpenAI has unveiled GPT-6 Astra, a frontier AI model the company says can identify zero-day vulnerabilities and create working proof-of-concept exploits during authorized cybersecurity tests.

Chaotic Eclipse Claims Avast Antivirus 0-Day Vulnerability – PoC Released

Cyber Security News - 03 September 2026 15:47

Researcher Chaotic Eclipse has claimed to have discovered a zero-day privilege-escalation vulnerability affecting Avast Antivirus and released a public proof-of-concept repository named PrettyPrague.

Attackers exploit zero-days in consistently besieged SonicWall product

CyberScoop - 03 September 2026 23:12

SonicWall customers have confronted a barrage of attacks for years, including five actively exploited vulnerabilities in SMA 1000 appliances since late 2025.

CC-4841 - Broadcom Releases Security Advisory for Critical Vulnerabilities in VMware Workstation and VMware Fusion

NHS Digital - 03 September 2026 14:57

Severity: Medium Security advisory addresses vulnerabilities that could lead to arbitrary code execution on a host system from an affected virtual machine.

HPE patches critical ArubaOS-CX remote code execution flaw

BleepingComputer - 03 September 2026 15:28

Hewlett Packard Enterprise (HPE) has patched a critical vulnerability in the ArubaOS-CX network operating system that could lead to remote code execution. [...]

Scottish Cyber Coordination Centre

Critical Elementor Pro flaw exploited to take over WordPress sites

BleepingComputer - 03 September 2026 11:52

A recently patched critical vulnerability (CVE-2026-32475) in the Elementor Pro plugin for WordPress is being exploited in attacks that deliver a webshell payload and execute arbitrary commands on the server. [...]

Critical Cisco Nexus 9000 Flaw Lets Unauthenticated Remote Attackers Run Code as Root

The Hacker News - 03 September 2026 22:22

Cisco has released patches to address a critical security flaw affecting 10 Silicon One-based Nexus 9000 switches that could allow an unauthenticated, remote attacker to execute code as root, alongside an IOS XR hardening release bundling 7 umbrella CVEs, 2 of which are rated 9.8, with no workaround for any IOS XR version.

Cisco searched for IOS XR bugs and found so many it rolled them into an update release

The Register - 04 September 2026 05:18

Three critical vulns demand your attention, one a make-me-root mess in Nexus 9000 Series Switches that you can mitigate, not fix

Threat actors and malware

LLMjacking Attack Uses Leaked AWS IAM Key to Steal Paid AI Model Access

Cyber Security News - 03 September 2026 17:58

A newly documented cloud intrusion shows how quickly attackers can turn a single leaked AWS credential into a revenue stream by hijacking access to premium AI models, a technique researchers call LLMjacking.

Phantom Deal Hackers Impersonate Executives and Use Fake NDAs to Steal Corporate Wire Transfers

Cyber Security News - 03 September 2026 16:01

Cybercriminals are using fake acquisition deals to steer employees toward large wire transfers.

Hackers Weaponize ScreenConnect to Spread Worm-Like Malware Across Windows Systems

Cyber Security News - 03 September 2026 15:52

Hackers are turning rogue remote-support installations into a tool that can spread malicious code between Windows computers.

Attackers exploit zero-days in consistently besieged SonicWall product

CyberScoop - 03 September 2026 23:12

Scottish Cyber Coordination Centre

SonicWall customers have confronted a barrage of attacks for years, including five actively exploited vulnerabilities in SMA 1000 appliances since late 2025.

2,000 Leaked Documents Reveal How Russia Turns Engineering Students Into GRU Cyber Operators

Security Affairs - 03 September 2026 09:12

2,000 leaked files expose Bauman University's hidden Department No. 4, which trained GRU-linked hackers and propagandists linked to APT28 and Sandworm.

Attackers Turn Trusted Node.js Runtime Into Malware Delivery Tool in Targeted Attacks

The Hacker News - 03 September 2026 17:13

Threat actors are leveraging the trusted Node.js JavaScript runtime in multiple cyber attacks as a way to deploy malicious payloads.

AI 'Machine Speed' Cuts 2-Week Attack Down to 10 Hours

darkreading - 03 September 2026 15:38

The incident demonstrates how frontier AI agents can dramatically compress an attack timeline and coordinate a large-scale breach, according to researchers.