



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

23 September 2026

Vulnerabilities

[Chrome Patches 108 Vulnerabilities Including Critical Flaws that Enable Code Execution Attacks](#)

Cyber Security News - 23 September 2026 08:46

Google has released Chrome 154 for Windows, macOS, and Linux, fixing 108 security vulnerabilities, including several critical memory-safety flaws that could potentially allow attackers to execute code through malicious web content.

[CC-4856 - Proof-of-Concept Exploit Code Released for Veeam Vulnerability CVE-2026-32996](#)

NHS Digital - 22 September 2026 15:00

Severity: Medium Exploitation of Veeam Agent for Microsoft Windows vulnerability could allow local privilege escalation to SYSTEM privileges Exploitation of Veeam Agent for Microsoft Windows vulnerability could allow local privilege escalation to SYSTEM privileges Updated: 22 Sep 2026

[F5 patches BIG-IP APM zero-day flaw exploited in RCE attacks](#)

BleepingComputer - 23 September 2026 04:17

F5 has released security updates to address a critical BIG-IP APM zero-day vulnerability being exploited in remote code execution attacks. [...]

[D-Link warns of max severity zero-day bug in DIR-822A routers](#)

BleepingComputer - 22 September 2026 09:48

D-Link warned customers of a maximum-severity vulnerability (CVE-2026-86296) with public proof-of-concept (PoC) exploit code and no patch, affecting legacy DIR-822A dual-band Wi-Fi routers. [...]

[WordPress Issues Patch for Critical Flaw That Can Enable Code Execution on Some Servers](#)

The Hacker News - 23 September 2026 00:33

WordPress has fixed a critical flaw in its core software that lets an attacker with no account make a site load a PHP file from outside its theme folders. On some servers, that can go further, allowing the attacker to run their own code.

[New CVSS 10.0 VeloCloud Orchestrator Flaw Actively Exploited in Certificate-Based Setups](#)



Scottish
Cyber
Coordination
Centre

The Hacker News - 22 September 2026 18:59

Attackers are exploiting a new flaw in on-premises VeloCloud Orchestrator (VCO), the server that manages the Edge devices in a VeloCloud SD-WAN, Arista said on September 22.

New Linux Kernel Flaw Gives ARM64 KVM Guests Read-Write Access to Host Memory

The Hacker News - 22 September 2026 18:08

A new flaw in the Linux kernel's KVM virtualization code for ARM64 processors can leave a freed piece of host memory exposed to a guest virtual machine on hosts with nested virtualization enabled.

NightmareEclipse's latest zero-day leaves Microsoft Defender stuck in the past

The Register - 22 September 2026 19:36

BigDiskBuster leaves Microsoft's antivirus running but unable to install updates

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-2026-85102 Check Point Multiple Products Improper Certificate Validation Vulnerability CVE-2026-93616 Check Point Multiple Products Path Traversal Vulnerability CVE-2026-93952 Arista VeloCloud Orchestrator Improper Input Validation Vulnerability CVE-2026-94127 F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability.

Threat actors and malware

ChatGPT Computer History Feature Creates New Attack Surface for macOS Infostealers

Cyber Security News - 23 September 2026 08:31

A new feature in ChatGPT now records your actions on your Mac, creating a detailed, plain-text diary of your work.

Hackers Exploiting F5 BIG-IP OAuth Server 0-day Flaw to Gain Remote Code Execution

Cyber Security News - 23 September 2026 04:24

F5 has warned that hackers are actively exploiting a critical zero-day vulnerability in BIG-IP Access Policy Manager (APM) deployments to execute code remotely without authentication. Tracked as CVE-2026-94127, the flaw affects virtual servers configured with both an APM access policy and an OAuth profile, specifically where APM operates as an OAuth Authorization Server..

ShinyHunters claims attack on FBI exposes almost all agents

CyberScoop - 23 September 2026 00:47



Scottish
Cyber
Coordination
Centre

The FBI jobs site, which was temporarily defaced, remains unavailable and the agency said it's investigating the claims.

Volexity spots another China-aligned threat group exploiting Chrome and Microsoft defects

CyberScoop - 22 September 2026 19:47

The threat group Volexity tracks as UTA0565 showcased a variance in tactics, but it used the same exploit kit as multiple Chinese threat groups.

Shai-Hulud Attack Nips Cyber-Firm CrowdSec's GitHub Data

darkreading - 22 September 2026 18:32

Threat actors stole 170 private repositories using an OAuth token stolen from a former employee's computer through the TanStack npm supply chain attack.

UK related

UK cops arrest 2 EvilTokens suspects, Microsoft seizes 50 phishing kit websites

The Register - 22 September 2026 18:00

Used by crims to compromise 12K+ email inboxes across 10K+ global orgs

UK to fight Russian disinformation and push new global AI standards, Burnham says

BBC News - 23 September 2026 08:07

The UK could act as "an honest broker" on AI and other global challenges, the prime minister tells world leaders at the UN.