



Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

24 September 2026

Vulnerabilities

[Check Point warns of hackers exploiting Security Gateway VPN RCE flaw](#)

BleepingComputer - 23 September 2026 16:53

Cybersecurity company Check Point has confirmed active exploitation of CVE-2026-85102, a pre-authentication remote code execution (RCE) vulnerability in the VPN certificate-handling functionality of its Security Gateway product.

[U.S. CISA adds Check Point, Arista VeloCloud Orchestrator, and F5 BIG-IP APM flaws to its Known Exploited Vulnerabilities catalog](#)

Security Affairs - 23 September 2026 21:37

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Check Point, Arista VeloCloud Orchestrator, and F5 BIG-IP APM flaws to its Known Exploited Vulnerabilities catalog.

[F5 BIG-IP APM Zero-Day Exploited in Zero-Day RCE Attacks](#)

Security Affairs - 23 September 2026 19:12

F5 warns of a critical BIG-IP APM zero-day, CVE-2026-94127, allowing remote code execution. Attackers are already exploiting it. F5 has released emergency security updates for a critical vulnerability, tracked as CVE-2026-94127 (CVSS score of 9.8), in BIG-IP Access Policy Manager (APM) that attackers are already exploiting in the wild.

[New cPanel Flaw Lets a Hosting Account Run Code as Root, Take Full Server Control](#)

The Hacker News - 23 September 2026 18:46

A flaw in cPanel's CalDAV and CardDAV service lets anyone with a cPanel hosting account run code as root and take "full control of the server".

[Adobe Patches Critical Flaws in Connect, AEM Forms](#)

SecurityWeek - 23 September 2026 12:40

The nine critical security defects could be exploited for arbitrary code execution and privilege escalation. The post Adobe Patches Critical Flaws in Connect, AEM Forms appeared first on SecurityWeek.

[Chrome 154 Patches 108 Vulnerabilities](#)

SecurityWeek - 23 September 2026 11:36

The browser update resolves several critical-severity memory safety and memory corruption flaws. The post Chrome 154 Patches 108 Vulnerabilities appeared first on SecurityWeek.



Scottish
Cyber
Coordination
Centre

Arista Urges Immediate Patching of Exploited VCO Zero-Day

SecurityWeek - 23 September 2026 09:33

Remote attackers could trigger the critical-severity flaw to access privileged internal functionality.

Threat actors and malware

Placeholder domain used in dev docs now serves ClickFix attacks

BleepingComputer - 23 September 2026 19:46

The "third-party.com" domain, commonly used as a placeholder in developer documentation and code examples, is serving a fake Cloudflare verification page that attempts to trick Windows users into executing PowerShell commands.

New RemControl Android banking malware targets users in Europe and Canada

BleepingComputer - 23 September 2026 18:25

A new Android malware-as-a-service (MaaS) platform called RemControl is targeting users through malvertising campaigns that impersonate the TVTap IPTV application.

Hackers start exploiting critical WordPress flaw for code execution

BleepingComputer - 23 September 2026 15:31

Threat actors have moved from probing WordPress sites vulnerable to CVE-2026-87902 to exploiting the flaw to write files to disk that execute shell commands when accessed.

CLOSEDQUORUM, the malware that asks four AI models what to do next

Security Affairs - 24 September 2026 06:44

Cisco Talos finds CLOSEDQUORUM, malware that lets four commercial AI models vote on its next move, with no human operator required. Cisco Talos found malware, dubbed CLOSEDQUORUM, that holds a vote before deciding what to steal from you.

Chinese Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy CLEANGULP Malware

The Hacker News - 23 September 2026 14:59

A Chinese threat actor codenamed UTA0565 has been observed exploiting the recently disclosed Google Chrome-Microsoft Windows exploit chain as zero-days through fake websites.