Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 May 2026

Vulnerabilities

Palo Alto PAN-OS Flaw Under Active Exploitation Enables Remote Code Execution

The Hacker News - 06 May 2026 12:44

Palo Alto Networks has released an advisory warning that a critical buffer overflow vulnerability in its PAN-OS software has been exploited in the wild. The vulnerability, tracked as CVE-2026-0300, has been described as a case of unauthenticated remote code execution.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2026-0300 Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability

Critical vm2 sandbox bug lets attackers execute code on hosts

BleepingComputer - 06 May 2026 15:38

A critical vulnerability in the popular Node.js sandboxing library vm2 allows escaping the sandbox and executing arbitrary code on the host system.

New Cisco DoS flaw requires manual reboot to revive devices

BleepingComputer - 06 May 2026 15:06

Cisco patched a Crosswork Network Controller and Network Services Orchestrator denial-of-service vulnerability that requires manually rebooting targeted systems for recovery.

Apache fixes critical HTTP/2 double-free flaw CVE-2026-23918 enabling RCE

Security Affairs - 06 May 2026 12:00

The Apache Software Foundation has released updates to fix multiple vulnerabilities in its HTTP Server, including CVE-2026-23918 (CVSS score of 8.8).

Threat actors and malware

MuddyWater hackers use Chaos ransomware as a decoy in attacks

BleepingComputer - 06 May 2026 10:02

The MuddyWater Iranian hackers disguised their operations as a Chaos ransomware attack, relying on Microsoft Teams social engineering to gain access and establish persistence.

Scottish Cyber Coordination Centre

Mirai-Based xlabs_v1 Botnet Exploits ADB to Hijack IoT Devices for DDoS Attacks

The Hacker News - 07 May 2026 02:51

Cybersecurity researchers have exposed a new Mirai-derived botnet that self-identifies as xlabs_v1 and targets internet-exposed devices running Android Debug Bridge (ADB) to enlist them in a network capable of carrying out distributed denial-of-service (DDoS) attacks.

DAEMON Tools devs confirm breach, release malware-free version

BleepingComputer - 06 May 2026 13:43

Disc Soft Limited, the maker of DAEMON Tools Lite, confirmed that the software had been trojanized in a supply chain attack and released a new, malware-free version.

Sophisticated Quasar Linux RAT Targets Software Developers

SecurityWeek - 06 May 2026 10:48

The persistent, evasive implant provides remote access, surveillance, and credential exfiltration capabilities.

Hackers abuse Google ads for GoDaddy ManageWP login phishing

BleepingComputer - 06 May 2026 18:36

A phishing campaign delivered through Google sponsored search results is targeting credentials for ManageWP, GoDaddy's platform for managing fleets of WordPress websites.

CloudZ Malware Abuses Phone Link to Steal SMS OTPs

Infosecurity Magazine - 06 May 2026 16:00

Cisco Talos uncovers CloudZ RAT and Pheno plugin abusing Microsoft Phone Link to intercept SMS OTPs