Scottish Cyber Coordination Centre

Daily Threat Bulletin

5 May 2026

Vulnerabilities

Weaver E-cology critical bug exploited in attacks since March

BleepingComputer - 04 May 2026 19:12

Hackers have been exploiting a critical vulnerability (CVE-2026-22679) in the Weaver E-cology office automation since mid-March to run discovery commands. [...]

Progress warns of critical MOVEit Automation auth bypass flaw

BleepingComputer - 04 May 2026 09:18

Progress Software warned customers to patch a critical authentication bypass vulnerability in its MOVEit Automation enterprise-grade managed file transfer (MFT) application. [...]

Hackers target governments and MSPs via critical cPanel flaw CVE-2026-41940

Security Affairs - 04 May 2026 20:10

Attackers exploit a critical cPanel flaw to target government and MSP networks across Southeast Asia and several countries, including the U.S. and Canada. A threat actor is exploiting critical cPanel vulnerability CVE-2026-41940 to target government and military organizations in Southeast Asia, along with MSPs and hosting providers in countries like the Philippines, Laos, Canada, South [...]

U.S. CISA adds a flaw in Linux Kernel to its Known Exploited Vulnerabilities catalog

Security Affairs - 04 May 2026 11:26

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a flaw in Linux Kernel to its Known Exploited Vulnerabilities catalog The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a flaw in the Linux Kernel, tracked as CVE-2026-31431 (CVSS score of 7.8), to its Known Exploited Vulnerabilities (KEV) catalog. Recently, Xint Code researchers warned of a serious Linux [...]

Threat actors and malware

Trellix discloses data breach after source code repository hack

BleepingComputer - 04 May 2026 13:25

Cybersecurity firm Trellix disclosed a data breach after attackers gained access to “a portion” of its source code repository. [...]

Phishing Campaign Hits 80+ Orgs Using SimpleHelp and ScreenConnect RMM Tools

The Hacker News - 05 May 2026 00:36

Scottish Cyber Coordination Centre

An active phishing campaign has been observed targeting multiple vectors since at least April 2025 with legitimate Remote Monitoring and Management (RMM) software as a way to establish persistent remote access to compromised hosts.The activity, codenamed VENOMOUS#HELPER, has impacted over 80 organizations, most of which are in the U.S., according to Securonix. It shares overlaps with clusters

The Coming Wave of Large-Scale AI-Enabled Cyberattacks

Security Magazine - 04 May 2026 13:00

The first truly major AI-enabled cyberattack will look different from the incidents that dominate headlines today.

Cybersecurity Professionals Sentenced to Prison for Ransomware Attacks

Security Magazine - 04 May 2026 12:00

Two cybersecurity professionals were imprisoned for their role in a string of 2023 ransomware attacks.

Exploit Cyber-Frenzy Threatens Millions via Critical cPanel Vulnerability

darkreading - 04 May 2026 20:14

Shortly after the authentication-bypass flaw was disclosed multiple proof-of-concept exploits appeared, and one researcher claims there's been zero-day activity for at least a month.

DigiCert Revokes Certificates After Support Portal Hack

SecurityWeek - 04 May 2026 13:46

Hackers delivered malware via a customer chat channel, infected an analyst's system, and accessed the internal support portal.The post DigiCert Revokes Certificates After Support Portal Hack appeared first on SecurityWeek.