Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 May 2026

Vulnerabilities

Google accidentally exposed details of unfixed Chromium flaw

BleepingComputer - 21 May 2026 15:13

Google has accidentally leaked details about an unfixed issue in Chromium that keeps JavaScript running in the background even when the browser is closed, allowing remote code execution on the device. [...]

Max severity Cisco Secure Workload flaw gives Site Admin privileges

BleepingComputer - 21 May 2026 10:58

Cisco has released security updates to address a maximum-severity vulnerability in Secure Workload that allows attackers to gain Site Admin privileges. [...]

Microsoft warns of new Defender zero-days exploited in attacks

BleepingComputer - 21 May 2026 04:49

On Wednesday, Microsoft started rolling out security patches for two Defender vulnerabilities that have been exploited in zero-day attacks. [...]

Cisco fixed maximum severity flaw CVE-2026-20223 in Secure Workload

Security Affairs - 21 May 2026 14:22

Cisco fixed a critical Secure Workload flaw (CVE-2026-20223) that could let attackers gain Site Admin privileges through crafted API requests. Cisco released patches for a critical vulnerability, tracked as CVE-2026-20223 (CVSS score of 10.0), in Secure Workload.

Highly Critical Drupal Core Flaw Exposes PostgreSQL Sites to RCE Attacks

The Hacker News - 21 May 2026 10:14

Drupal has released security updates for a “highly critical” security vulnerability in Drupal Core that could be exploited by attackers to achieve remote code execution, privilege escalation, or information disclosure.The vulnerability, now tracked as CVE-2026-9082, carries a CVSS score of 6.5 out of 10.0, per CVE.org.

Threat actors and malware

GitHub links repo breach to TanStack npm supply-chain attack

BleepingComputer - 21 May 2026 03:54

GitHub says the hackers who breached 3,800 internal repositories gained access via a malicious version of the Nx Console VS Code extension, compromised in last week's TanStack npm supply-chain attack. [...]

Attackers are bypassing MFA on SonicWall VPNs because something was wrong with previous fix

Security Affairs - 21 May 2026 15:29

Attackers bypassed MFA on patched SonicWall Gen6 VPNs because admins missed extra manual steps required to fully fix the flaw. There is a particular kind of security failure that is harder to catch than an unpatched system: a patched system where the patch did not actually work because nobody followed all the steps.

AI Is Expanding the Enterprise Data Leakage Attack Surface

Security Boulevard - 21 May 2026 19:00

The promise of AI is real: faster decisions, competitive advantage, and innovation at a pace that was not possible two years ago. Every enterprise technology leader I speak with feels it. The pressure to deploy, operationalize, and not fall behind is relentless. But there is a critical risk hidden within all of that momentum.

Mini Shai-Hulud: Frequently asked questions about the TeamPCP npm and PyPI supply chain campaign

Security Boulevard - 21 May 2026 16:28

A self-propagating worm has compromised more than 170 npm and PyPI packages, defeating provenance attestation and breaching OpenAI and Mistral AI. Here is what you need to know.Key takeawaysMini Shai-Hulud is a self-propagating worm by TeamPCP that steals developer and cloud credentials across the npm and PyPI ecosystems.