Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 June 2026

Vulnerabilities

CC-4790 - Active Exploitation of Authentication Bypass Vulnerability in Palo Alto Network's PAN-OS GlobalProtect

NHS Digital - 01 June 2026 13:30

Severity: Medium Successful exploitation of CVE-2026-0257 allows unauthenticated attackers to establish unauthorised VPN connections via affected PAN-OS GlobalProtect deployments. Successful exploitation of CVE-2026-0257 allows unauthenticated attackers to establish unauthorised VPN connections via affected PAN-OS GlobalProtect deployments.

Critical Windows Netlogon RCE flaw now exploited in attacks

BleepingComputer - 01 June 2026 09:30

The Centre for Cybersecurity Belgium (CCB), the country's national authority for cybersecurity, warned on Friday that threat actors are now exploiting a recently patched critical Windows Netlogon vulnerability in attacks. [...]

CVE-2026-8732: The WP Maps Pro Flaw That Lets Anyone Create a WordPress Admin Without a Password

Security Affairs - 01 June 2026 12:36

CVE-2026-8732 in WP Maps Pro lets unauthenticated attackers create WordPress admin accounts. 2,858 attacks blocked in 24 hours. WP Maps Pro plugin allows WordPress site owners to embed Google Maps and OpenStreetMap with markers, listings, and location search. It's a store locator tool. Unremarkable.

CIFSwitch, a Linux Root Bug Hidden in Plain Sight for 19 Years

Security Affairs - 01 June 2026 10:55

CIFSwitch is a 19-year-old Linux logic bug turning forged CIFS auth keys into root. Affects Mint, CentOS, Rocky, Kali, SLES. CIFSwitch stands apart from typical privilege escalation vulnerabilities because of how it was discovered. Asim Manizada, a security engineer at SpaceX, didn't find it by auditing source code the old-fashioned way.

Threat actors and malware

Hackers hijack thousands of sites for ClickFix and FakeUpdate attacks

BleepingComputer - 01 June 2026 19:14

A threat actor tracked as DriveSurge has been operating large-scale malware distribution campaigns using ClickFix and FakeUpdates techniques on compromised sites. [...]

Scottish Cyber Coordination Centre

Dashlane password manager users locked out by brute force attacks

BleepingComputer - 01 June 2026 15:17

Multiple Dashlane users have been locked out of their accounts following brute-force attacks that attempted logins from distant locations and unknown devices. [...]

WordPress malware campaign hides payloads in Steam profiles

BleepingComputer - 01 June 2026 14:04

Nearly 2,000 WordPress websites were infected with malware that relies on Steam Community profile comments to hide command-and-control (C2) data. [...]

Miasma Supply Chain Attack Compromises Red Hat npm Packages with Credential-Stealing Worm

The Hacker News - 02 June 2026 00:10

A new Mini Shai-Hulud supply chain attack campaign, codenamed Miasma, has compromised @redhat-cloud-services packages to steal credentials and secrets from developer machines and deliver a self-propagating worm.

OpenAI Codex Authentication Tokens Stolen in codexui-android npm Supply Chain Attack

The Hacker News - 01 June 2026 16:01

Cybersecurity researchers have disclosed details of a new malicious supply chain campaign that's targeting developers using OpenAI Codex through a legitimate-looking remote web UI.The tool, named codexui-android, is advertised on GitHub and npm as a remote web UI for OpenAI Codex, attracting over 29,000 weekly downloads. The package is still available for download from the repository.