Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 June 2026

Vulnerabilities

CISA warns of another cPanel plugin flaw exploited in attacks

BleepingComputer - 16 June 2026 07:47

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has given U.S. government agencies three days to secure their servers against an actively exploited vulnerability (CVE-2026-54420) in the LiteSpeed cPanel user-end plugin. [...]

CVE-2026-20262: CISCO Catalyst SD-WAN Flaw Under Active Targeted Exploitation

Security Affairs - 16 June 2026 11:53

Cisco warned that CVE-2026-20262, a Catalyst SD-WAN Manager vulnerability allowing arbitrary file writes, is being actively exploited. Cisco confirmed active exploitation of CVE-2026-20262, an arbitrary file write vulnerability affecting Catalyst SD-WAN Manager. CVE-2026-20262 (CVSS score of 6.5) is an arbitrary file write vulnerability in the web interface of Cisco Catalyst SD-WAN Manager.

Google Vertex AI SDK Flaw Let Attackers Hijack Model Uploads via Bucket Squatting

The Hacker News - 17 June 2026 01:35

A flaw in the Google Cloud Vertex AI SDK for Python let an attacker with no access to a victim's project hijack the victim's machine learning model upload and run code inside Google's serving infrastructure.

Attackers Exploit Three Fortinet FortiSandbox Flaws, One Patched Last Week

The Hacker News - 16 June 2026 17:00

Bad actors are exploiting multiple security vulnerabilities in Fortinet FortiSandbox, according to threat intelligence firm Defused Cyber.

LiteLLM Vulnerability Chain Lets Low-Privilege Users Take Over AI Gateway Servers

The Hacker News - 15 June 2026 23:09

A default low-privilege account on a LiteLLM proxy can climb to full admin and run code on the server by chaining three vulnerabilities, researchers at Obsidian Security disclosedLiteLLM is a widely deployed open-source AI gateway that brokers calls to more than 100 model providers behind one OpenAI-compatible interface.

Threat actors and malware

New Rokarolla Android malware targets 217 banking, crypto apps

Scottish Cyber Coordination Centre

BleepingComputer - 16 June 2026 17:04

A new Android banking trojan named Rokarolla is targeting 217 banking and cryptocurrency applications using an extensive set of 137 commands. [...]

GhostTree Attack Abused Recursive Windows Junctions to Hide Malware

BleepingComputer - 16 June 2026 11:17

GhostTree uses recursive NTFS junctions to generate vast numbers of valid Windows file paths. Varonis explains how the technique could cause Microsoft Defender folder scans to never complete, leaving malware undetected. [...]

Windows version of SprySOCKS Linux malware used to attack govt orgs

BleepingComputer - 16 June 2026 06:00

Windows variants for the SprySOCKS Linux malware have been used in attacks targeting government organizations in at least four countries. [...]

China-linked actor spent two years inside medical research networks

Security Affairs - 16 June 2026 08:32

China's UNC6508 hid in North American medical research networks for 2 years, stealing credentials and forwarding emails to Gmail Google's Threat Intelligence Group published a report this week on UNC6508, a China-linked cyberespionage group that breached North American medical and military research organizations and stayed hidden for more than two years.

ClickFix Campaigns Expand Malware Delivery With New Loaders and Fake Update Lures

The Hacker News - 17 June 2026 00:11

Cybersecurity researchers have flagged multiple ClickFix campaigns that deliver three malware loaders called BabaDeda Loader, Lorem Ipsum Loader, and Potemkin, per independent reports from Morphisec, BlueVoyant, and Huntress, respectively.Attacks involving BabaDeda Loader, observed in April 2026, have targeted education and financial organizations.

New Rokarolla Android Malware Steals PINs, SMS Codes, and Crypto Wallet Funds

The Hacker News - 16 June 2026 19:40

Security researchers at Zimperium's zLabs have documented a new Android banking trojan, Rokarolla, that targets 217 banking and cryptocurrency apps and packs 137 remote commands.

UK related

UK to require ID or face scan before you can make social media accounts

BleepingComputer - 16 June 2026 11:38

Scottish Cyber Coordination Centre

Opening a new social media account in the UK will soon mean proving you're over 16 with an ID upload or a facial age scan, under a government ban on under-16s taking effect in spring 2027. Security experts warn the age checks are easy to circumvent and create new data-breach risks. [...]