Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 April 2026

Vulnerabilities

LMDeploy CVE-2026-33626 Flaw Exploited Within 13 Hours of Disclosure

The Hacker News - 24 April 2026 13:54

A high-severity security flaw in LMDeploy, an open-source toolkit for compressing, deploying, and serving large language models (LLMs), has come under active exploitation in the wild less than 13 hours after its public disclosure.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2024-7399 Samsung MagicINFO 9 Server Path Traversal Vulnerability
CVE-2024-57726 SimpleHelp Missing Authorization Vulnerability
CVE-2024-57728 SimpleHelp Path Traversal Vulnerability
CVE-2025-29635 D-Link DIR-823X Command Injection Vulnerability

Over 400,000 sites at risk as hackers exploit Breeze Cache plugin flaw (CVE-2026-3844)

Security Affairs - 25 April 2026 15:22

Threat actors are exploiting a critical flaw, tracked as CVE-2026-3844 (CVSS score of 9.8), in the Breeze Cache WordPress plugin, allowing them to upload files to a server without authentication.

New 'Pack2TheRoot' flaw gives hackers root Linux access

BleepingComputer - 24 April 2026 14:28

A new vulnerability dubbed Pack2TheRoot could be exploited in the PackageKit daemon to allow local Linux users to install or remove system packages and gain root permissions.

Critical bug in CrowdStrike LogScale let attackers access files

Security Affairs - 26 April 2026 17:07

CrowdStrike recently disclosed a critical vulnerability, tracked as CVE-2026-40050, affecting its LogScale self-hosted product. The flaw enables unauthenticated path traversal, which could allow a remote attacker to read arbitrary files from the server filesystem.

Scottish Cyber Coordination Centre

Threat actors and malware

Threat actor uses Microsoft Teams to deploy new "Snow" malware

BleepingComputer - 25 April 2026 12:07

A threat group tracked as UNC6692 uses social engineering to deploy a new, custom malware suite named 'Snow' which includes a browser extension, a tunneler, and a backdoor.

ADT confirms data breach after ShinyHunters leak threat

BleepingComputer - 24 April 2026 19:53

Home security giant ADT has confirmed a data breach after the ShinyHunters extortion group threatened to leak stolen data unless a ransom is paid.

Firestarter malware survives Cisco firewall updates, security patches

BleepingComputer - 24 April 2026 17:34

Cybersecurity agencies in the U.S. and U.K. are warning about a custom malware called Firestarter persisting on Cisco Firepower and Secure Firewall devices running Adaptive Security Appliance (ASA) or Firepower Threat Defense (FTD) software.

North Korea's Lazarus Targets macOS Users via ClickFix

darkreading - 24 April 2026 14:00

Lazarus continues leveraging ClickFix for initial access and data theft, in this case, against Mac-centric organizations and their high-value leaders.

Pre-Stuxnet Sabotage Malware 'Fast16' Linked to US-Iran Cyber Tensions

SecurityWeek - 24 April 2026 15:57

It targeted high-precision calculation software to tamper with results and packed a self-propagation mechanism.

UK incidents

UK Biobank Data Breach: Health Data of 500,000 Listed for Sale in China

Infosecurity Magazine - 24 April 2026 14:25

UK government Minister confirms that breached health records of UK Biobank volunteers were up for sale on Chinese ecommerce platforms before being removed.