Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 May 2026

Vulnerabilities

Preparing for a 'vulnerability patch wave'

NCSC - 01 May 2026 13:00

Organisations must act now to prepare for a wave of patches that will address decades of technical debt.

Critrical cPanel flaw mass-exploited in "Sorry" ransomware attacks

BleepingComputer - 02 May 2026 18:54

A new disclosed cPanel flaw tracked as CVE-2026-41940 is being mass-exploited to breach websites and encrypt data in "Sorry" ransomware attacks. [...]

Google Revamps Bug Bounty Programs: Android Rewards Rise, Chrome Payouts Drop in the Age of AI

Security Affairs - 03 May 2026 09:25

Google revamps bug bounties: Android rewards rise to $1.5M, Chrome payouts drop, shifting focus to high-impact, AI-resistant vulnerabilities. Google has announced a major overhaul of its Vulnerability Reward Programs (VRP) for Android and Chrome, marking a strategic shift in how the company approaches cybersecurity. The update comes as artificial intelligence tools are reshaping the field [...]

CISA Adds Actively Exploited Linux Root Access Bug CVE-2026-31431 to KEV

The Hacker News - 03 May 2026 12:56

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added a recently disclosed security flaw impacting various Linux distributions to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild

Poisoned Ruby Gems and Go Modules Exploit CI Pipelines for Credential Theft

The Hacker News - 01 May 2026 16:13

A new software supply chain attack campaign has been observed using sleeper packages as a conduit to subsequently push malicious payloads that enabled credential theft, GitHub Actions tampering, and SSH persistence.

Anthropic Rolls Out Claude Security for AI Vulnerability Scanning

Infosecurity Magazine - 01 May 2026 13:00

Claude Security enters public beta, giving enterprises AI driven code scanning with no API integration or custom agents required

Scottish Cyber Coordination Centre

Threat actors and malware

Instructure confirms data breach, ShinyHunters claims attack

BleepingComputer - 03 May 2026 19:16

Educational tech giant Instructure has confirmed that data was stolen in a cyberattack, with the ShinyHunters extortion gang claiming responsibility. [...]

ConsentFix v3 attacks target Azure with automated OAuth abuse

BleepingComputer - 02 May 2026 11:32

A new attack type, dubbed ConsentFix v3, has been circulating on hacker forums, building on the previous technique by adding automation and scaling potential. [...]

New Deep#Door RAT uses stealth and persistence to target Windows

Security Affairs - 02 May 2026 09:22

Deep#Door hides a Python RAT inside a batch file, kills Windows defenses, survives via multiple persistence methods, and exfiltrates data through a public TCP tunnel. Security researchers at Securonix uncovered a sophisticated malware campaign called Deep#Door. Threat actors employed a stealthy Python-based backdoor that uses a surprisingly simple delivery method to achieve deep, persistent access [...]

Cybercrime Groups Using Vishing and SSO Abuse in Rapid SaaS Extortion Attacks

The Hacker News - 01 May 2026 20:56

Cybersecurity researchers are warning of two cybercrime groups that are carrying out “rapid, high-impact attacks” operating almost within the confines of SaaS environments, while leaving minimal traces of their actions.

1,800 Developers Hit in Mini Shai-Hulud Supply Chain Attack Across PyPI, NPM, and PHP

Security Boulevard - 03 May 2026 07:16

What happened A supply chain attack campaign attributed to TeamPCP, dubbed Mini Shai-Hulud, has compromised packages across the PyPI, NPM, and PHP ecosystems over a two-day period, affecting over 1,800 developer repositories containing stolen credentials.

UK related

Securing AI procurement and third-party models: a practical guide for UK SMEs

Security Boulevard - 03 May 2026 15:17

Securing AI procurement and third-party models: a practical guide for UK SMEs Third-party AI tools can be useful, but they also change the way your business handles data, makes decisions, and depends on suppliers. For many UK SMEs, the risk is not the model itself. It is

the way the tool is bought, connected, configured, [...]The post Securing AI procurement and third-party models: a practical guide for UK SMEs appeared first on Clear Path Security Ltd.