Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 April 2026

Vulnerabilities

Robinhood account creation flaw abused to send phishing emails

BleepingComputer - 27 April 2026 20:11

Online trading platform Robinhood's account creation process was exploited by threat actors to inject phishing messages into legitimate emails, tricking users into believing their accounts had suspicious activity. [...]

Firefox bug CVE-2026-6770 enabled cross-site tracking and Tor fingerprinting

Security Affairs - 27 April 2026 11:49

CVE-2026-6770 let attackers fingerprint Firefox and Tor users, even in Private mode. Firefox 150 and Tor Browser 15.0.10 fixed it. A vulnerability, tracked as CVE-2026-6770, allowed attackers to fingerprint Firefox users, even in Private Browsing, and also impacted the Tor Browser.

Microsoft Patches Entra ID Role Flaw That Enabled Service Principal Takeover

The Hacker News - 28 April 2026 13:07

An administrative role meant for artificial intelligence (AI) agents within Microsoft Entra ID could enable privilege escalation and identity takeover attacks, according to new findings from Silverfort.

Microsoft Confirms Active Exploitation of Windows Shell CVE-2026-32202

The Hacker News - 28 April 2026 12:20

Microsoft on Monday revised its advisory for a now-patched, high-severity security flaw impacting Windows Shell to acknowledge that it has been actively exploited in the wild.The vulnerability in question is CVE-2026-32202 (CVSS score: 4.3), a spoofing vulnerability that could allow an attacker to access sensitive information

Mythos Changed the Math on Vulnerability Discovery. Most Teams Aren't Ready for the Remediation Side

The Hacker News - 27 April 2026 18:28

Anthropic's Claude Mythos Preview has dominated security discussions since its April 7 announcement. Early reporting describes a powerful cybersecurity-focused AI system capable of identifying vulnerabilities at scale and raising serious questions about how quickly organizations can validate, prioritize, and remediate what it finds.

Threat actors and malware

Scottish Cyber Coordination Centre

GlassWorm malware attacks return via 73 OpenVSX “sleeper” extensions

BleepingComputer - 27 April 2026 18:41

A new wave of the Glassworm campaign is targeting the OpenVSX ecosystem with 73 “sleeper” extensions that turn malicious after an update. [...]

PyPI package with 1.1M monthly downloads hacked to push infostealer

BleepingComputer - 27 April 2026 12:17

An attacker pushed a malicious version of the popular elementary-data package Python Package Index (PyPI) to steal sensitive developer data and cryptocurrency wallets. [...]

Medtronic confirms breach after hackers claim 9 million records theft

BleepingComputer - 27 April 2026 10:50

Medical device giant Medtronic disclosed last week that hackers breached its network and accessed data in “certain corporate IT systems.” [...]

Checkmarx Confirms GitHub Repository Data Posted on Dark Web After March 23 Attack

The Hacker News - 27 April 2026 20:49

Checkmarx has disclosed that its ongoing investigation tied to the supply chain security incident has revealed that a cybercriminal group published data related to the company on the dark web.

Researchers Uncover 73 Fake VS Code Extensions Delivering GlassWorm v2 Malware

The Hacker News - 27 April 2026 17:53

Cybersecurity researchers have flagged dozens of Microsoft Visual Studio Code (VS Code) extensions on the Open VSX repository that are linked to a persistent information-stealing campaign dubbed GlassWorm.

Fake CAPTCHA IRSF Scam and 120 Keitaro Campaigns Drive Global SMS, Crypto Fraud

The Hacker News - 27 April 2026 13:03

Cybersecurity researchers have disclosed details of a telecommunications fraud campaign that uses fake CAPTCHA verification tricks to dupe unsuspecting users into sending international text messages that incur charges on their mobile bills, generating illicit revenue for the threat actors who lease the phone numbers.