Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 June 2026

Vulnerabilities

CISA sets urgent deadline to fix Cisco flaw exploited in attacks

BleepingComputer - 26 June 2026 16:43

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is giving federal agencies until Sunday to patch a vulnerability in Cisco Unified Communications Manager Server that is being actively exploited. [...]

DirtyClone: Fourth Linux Kernel Flaw in Six Weeks Escalates to Root

Security Affairs - 27 June 2026 10:12

DirtyClone: a Linux kernel privilege escalation that silently rewrites executables in memory, leaving no disk trace. Patch now. JFrog Security Research published a working exploit walkthrough on June 25 for CVE-2026-43503 (CVSS score of 8.8), a Linux kernel privilege escalation they call DirtyClone.

New Linux pedit COW Exploit Enables Root Access by Poisoning Cached Binaries

The Hacker News - 26 June 2026 20:27

A flaw in the Linux kernel's traffic-control subsystem can let a local unprivileged user gain root on affected systems.CVE-2026-46331, nicknamed "pedit COW," is an out-of-bounds write in the packet-editing action (act_pedit) that corrupts shared page-cache memory.

Amazon Q Developer Flaw Could Let Malicious Repos Run Code via MCP Configs

The Hacker News - 26 June 2026 20:23

A high-severity flaw in Amazon Q Developer let a malicious repository run commands and steal a developer's cloud credentials.

CISA Adds Exploited PTC Windchill RCE Flaw to KEV as Web Shell Attacks Continue

The Hacker News - 26 June 2026 19:01

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added a critical remote code execution vulnerability impacting PTC Windchill PDMlink and PTC FlexPLM enterprise Product Data Management (PDM) and Product Lifecycle Management (PLM) software to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Threat actors and malware

Clean GitHub repo tricks AI coding agents into running malware

BleepingComputer - 27 June 2026 11:22

An agentic coding tool tasked with cloning and setting up a seemingly benign GitHub repository could execute a malicious payload that remains invisible to security scanners, AI agents, and human reviewers. [...]

FBI: Russian hackers now target Signal backup recovery keys

BleepingComputer - 26 June 2026 19:06

The FBI and CISA are warning that a phishing campaign targeting Signal users tied to Russian intelligence services has evolved to steal Signal Backup Recovery Keys, allowing attackers to access victims' historical messages. [...]

Hospitality Sector Hit by Phishing Campaign Using Fake Guest Complaint Emails

Security Affairs - 27 June 2026 16:20

Microsoft warns of a phishing campaign targeting the hospitality sector with fake guest emails that install TonRAT using resilient persistence. Microsoft Threat Intelligence published a detailed analysis on an ongoing hacking campaign against hospitality organizations that has been running since April 2026.

New SharkLoader Malware Deploys Cobalt Strike in StrikeShark Cyberattacks

The Hacker News - 27 June 2026 00:47

A newly discovered cyber attack campaign has been observed delivering a previously undocumented malware family called SharkLoader that acts as a loader for deploying Cobalt Strike Beacon on compromised hosts.Kaspersky, which is tracking the activity under the moniker StrikeShark, said the campaign has targeted a diplomatic organization in Indonesia, government organizations in Taiwan,

China Announces Its Answer to Mythos With Its Own Cyber Weapon of Mass Destruction

Security Boulevard - 29 June 2026 03:50

Chinese AI company Qihoo 360 announced ithad developed an engine that can compete with Anthropic's Mythos artificialintelligence model. Mythos, which was introduced in early 2026, was transformative in finding cybersecurityvulnerabilities, developing exploits that can take advantage of thoseweaknesses, and chaining together vulnerabilities in ways humans cannot easilycomprehend, even those deemed as not important, into credible threats.

Miasma campaign poisons 20-plus npm packages, hunts for developer secrets

The Register - 26 June 2026 15:18

Microsoft says latest attack targets Leo Platform and RStreams packages, harvesting creds and going after more maintainers

Malware steals Chrome session cookies to take over your accounts

Malwarebytes - 26 June 2026 13:44

Scottish Cyber Coordination Centre

A phishing campaign installs a malicious Chrome extension to hijack browser sessions and compromise Windows devices.