Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

2 June 2025

Vulnerabilities

Exploit details for max severity Cisco IOS XE flaw now public

BleepingComputer - 31 May 2025 11:09

Technical details about a maximum-severity Cisco IOS XE WLC arbitrary file upload flaw tracked as CVE-2025-20188 have been made publicly available, bringing us closer to a working exploit. [...]

Two flaws in vBulletin forum software are under attack

Security Affairs - 01 June 2025 14:50

Experts found two vulnerabilities in the vBulletin forum software, one of which is already being exploited in real-world attacks. Two critical vBulletin flaws, tracked as CVE-2025-48827 and CVE-2025-48828, enable API abuse and remote code execution. The experts warn that one of these flaws is actively exploited in the wild. An unauthenticated user could exploit CVE-2025-48827 [...]

New Linux Flaws Allow Password Hash Theft via Core Dumps in Ubuntu, RHEL, Fedora

The Hacker News - 31 May 2025 16:49

Two information disclosure flaws have been identified in apport and systemd-coredump, the core dump handlers in Ubuntu, Red Hat Enterprise Linux, and Fedora, according to the Qualys Threat Research Unit (TRU).Tracked as CVE-2025-5054 and CVE-2025-4598, both vulnerabilities are race condition bugs that could enable a local attacker to obtain access to access sensitive information. Tools like

Threat actors and malware

Police takes down AVCheck site used by cybercriminals to scan malware

BleepingComputer - 30 May 2025 13:46

An international law enforcement operation has taken down AVCheck, a service used by cybercriminals to test whether their malware is detected by commercial antivirus software before deploying it in the wild. [...]

Germany doxxes Conti ransomware and TrickBot ring leader

BleepingComputer - 30 May 2025 12:57

The Federal Criminal Police Office of Germany (Bundeskriminalamt or BKA) claims that Stern, the leader of the Trickbot and Conti cybercrime gangs, is a 36-year-old Russian named Vitaly Nikolaevich Kovalev. [...]

Meta stopped covert operations from Iran, China, and Romania spreading propaganda

Security Affairs - 30 May 2025 21:02

Meta stopped three covert operations from Iran, China, and Romania using fake accounts to spread propaganda on social media platforms. Meta announced the disruption of three influence operations from Iran, China, and Romania using fake accounts to spread propaganda and manipulate discourse on Facebook, Instagram, and more.

Fake Recruiter Emails Target CFOs Using Legit NetBird Tool Across 6 Global Regions

The Hacker News - 02 June 2025 12:21

Cybersecurity researchers have warned of a new spear-phishing campaign that uses a legitimate remote access tool called Netbird to target Chief Financial Officers (CFOs) and financial executives at banks, energy companies, insurers, and investment firms across Europe, Africa, Canada, the Middle East, and South Asia.

New EDDIESTEALER Malware Bypasses Chrome's App-Bound Encryption to Steal Browser Data

The Hacker News - 30 May 2025 20:44

A new malware campaign is distributing a novel Rust-based information stealer dubbed EDDIESTEALER using the popular ClickFix social engineering tactic initiated via fake CAPTCHA verification pages.

China-Linked Hackers Exploit SAP and SQL Server Flaws in Attacks Across Asia and Brazil

The Hacker News - 30 May 2025 17:42

The China-linked threat actor behind the recent in-the-wild exploitation of a critical security flaw in SAP NetWeaver has been attributed to a broader set of attacks targeting organizations in Brazil, India, and Southeast Asia since 2023.

UK related

UK MoD Launches New Cyber Warfare Command

Infosecurity Magazine - 30 May 2025 10:00

The UK MoD has unveiled a new Cyber and Electromagnetic Command, which will focus on offensive cyber operations and “electromagnetic warfare” capabilities.