Scottish Cyber Coordination Centre

Daily Threat Bulletin

6 March 2026

Vulnerabilities

WordPress membership plugin bug exploited to create admin accounts

BleepingComputer - 05 March 2026 14:44

Hackers are exploiting a critical vulnerability in the User Registration & Membership plugin, which is installed on more than 60,000 WordPress sites. [...]

Google GTIG: 90 zero-day flaws exploited in 2025 as enterprise targets grow

Security Affairs - 06 March 2026 08:58

Google's GTIG reports 90 zero-day vulnerabilities exploited in the wild in 2025, up from 78 in 2024, with a growing share targeting enterprise systems. Google's Threat Intelligence Group (GTIG) identified 90 zero-day vulnerabilities exploited in the wild in 2025.

Hikvision and Rockwell Automation CVSS 9.8 Flaws Added to CISA KEV Catalog

The Hacker News - 06 March 2026 13:00

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added two security flaws impacting Hikvision and Rockwell Automation products to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Cisco Confirms Active Exploitation of Two Catalyst SD-WAN Manager Vulnerabilities

The Hacker News - 05 March 2026 21:52

Cisco has disclosed that two more vulnerabilities affecting Catalyst SD-WAN Manager (formerly SD-WAN vManage) have come under active exploitation in the wild.The vulnerabilities in question are listed below -CVE-2026-20122 (CVSS score: 7.1) - An arbitrary file overwrite vulnerability that could allow an authenticated, remote attacker to overwrite arbitrary files on the local file system.

Cisco Drops 48 New Firewall Vulnerabilities, 2 Critical

darkreading - 05 March 2026 21:11

Edge bugs are so fetch, and Cisco just dropped 50 new ones, including some heavy hitters with 10 out of 10 scores on the CVSS scale.

ContextCrush Flaw Exposes AI Development Tools to Attacks

Infosecurity Magazine - 05 March 2026 15:00

Critical flaw "ContextCrush" in Context7 MCP Server could allow malicious instructions into AI tools

Scottish Cyber Coordination Centre

Coruna Exploit Kit Targets Older iPhones in Multi-Stage Campaigns

Infosecurity Magazine - 05 March 2026 13:15

Exploit kit “Coruna” targets iPhones running iOS 13.0 to 17.2.1, focusing on financial data theft

Zero-Click FreeScout Bug Enables Remote Code Execution

Infosecurity Magazine - 05 March 2026 12:00

Ox Security warns that Mail2Shell could enable threat actors to hijack FreeScout systems without user interaction

Threat actors and malware

Chinese state hackers target telcos with new malware toolkit

BleepingComputer - 05 March 2026 19:19

A China-linked advanced persistent threat actor tracked as UAT-9244 has been targeting telecommunication service providers in South America since 2024, compromising Windows, Linux, and network-edge devices. [...]

Microsoft Reveals ClickFix Campaign Using Windows Terminal to Deploy Lumma Stealer

The Hacker News - 06 March 2026 13:14

Microsoft on Thursday disclosed details of a new widespread ClickFix social engineering campaign that has leveraged the Windows Terminal app as a way to activate a sophisticated attack chain and deploy the Lumma Stealer malware.

Europol-Led Operation Takes Down Tycoon 2FA Phishing-as-a-Service Linked to 64,000 Attacks

The Hacker News - 05 March 2026 13:21

Tycoon 2FA, one of the prominent phishing-as-a-service (PhaaS) toolkits that allowed cybercriminals to stage adversary-in-the-middle (AitM) credential harvesting attacks at scale, was dismantled by a coalition of law enforcement agencies and security companies.