Scottish Cyber Coordination Centre

Daily Threat Bulletin

30 March 2026

Vulnerabilities

U.S. CISA adds a flaw in F5 BIG-IP AMP to its Known Exploited Vulnerabilities catalog

Security Affairs - 28 March 2026 08:33

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a flaw in F5 BIG-IP AMP, tracked as CVE-2025-53521 (CVSS ver. 3.1 score of 9.8), to its Known Exploited Vulnerabilities (KEV) catalog.

Citrix NetScaler Under Active Recon for CVE-2026-3055 (CVSS 9.3) Memory Overread Bug

The Hacker News - 28 March 2026 15:41

A recently disclosed critical security flaw impacting Citrix NetScaler ADC and NetScaler Gateway is witnessing active reconnaissance activity, according to Defused Cyber and watchTowr. The vulnerability, CVE-2026-3055 (CVSS score: 9.3), refers to a case of insufficient input validation leading to memory overread, which an attacker could exploit to leak potentially sensitive information.

File read flaw in Smart Slider plugin impacts 500K WordPress sites

BleepingComputer - 29 March 2026 11:38

A vulnerability in the Smart Slider 3 WordPress plugin, active on more than 800,000 websites, can be exploited to allow subscriber-level users access to arbitrary files on the server.

TP-Link Patches High-Severity Router Vulnerabilities

SecurityWeek - 27 March 2026 12:42

The security defects could be used to bypass authentication, execute arbitrary commands, and decrypt configuration files.

Threat actors and malware

Cloudflare-Themed ClickFix Attack Drops Infiniti Stealer on Macs

SecurityWeek - 28 March 2026 11:30

The infection chain includes a fake CAPTCHA page, a Bash script, a Nuitka loader, and the Python-based infostealer.

Scottish Cyber Coordination Centre

Fake VS Code alerts on GitHub spread malware to developers

BleepingComputer - 27 March 2026 13:51

A large-scale campaign is targeting developers on GitHub with fake Visual Studio Code (VS Code) security alerts posted in the Discussions section of various projects, to trick users into downloading malware.

TA446 Deploys DarkSword iOS Exploit Kit in Targeted Spear-Phishing Campaign

The Hacker News - 28 March 2026 13:37

Proofpoint has disclosed details of a targeted email campaign in which threat actors with ties to Russia are leveraging the recently disclosed DarkSword exploit kit to target iOS devices. The activity has been attributed with high confidence to the Russian state-sponsored threat group known as TA446, which is also tracked by the broader cybersecurity community under the moniker Callisto.

ShinyHunters claims the hack of the European Commission

Security Affairs - 28 March 2026 16:58

The European Commission has allegedly been breached by ShinyHunters, with reported data dumps including content from mail servers and internal communications systems. The cybercrime group added the Commission to its Tor data leak site, claiming the theft of over 350 GB+ of data.