Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 March 2026

Vulnerabilities

New 'PolyShell' flaw allows unauthenticated RCE on Magento e-stores

BleepingComputer - 19 March 2026 17:01

A newly disclosed vulnerability dubbed 'PolyShell' affects all Magento Open Source and Adobe Commerce stable version 2 installations, allowing unauthenticated code execution and account takeover. [...]

Critical Ubiquiti UniFi UniFi security flaw allows potential account hijacking

Security Affairs - 19 March 2026 22:21

Ubiquiti fixed two UniFi vulnerabilities, including a critical flaw that could let attackers take over user accounts. Ubiquiti patched two vulnerabilities in its UniFi Network app, including a maximum-severity flaw that could enable account takeover.

U.S. CISA adds a flaw in Cisco FMC and Cisco SCC Firewall Management to its Known Exploited Vulnerabilities catalog

Security Affairs - 19 March 2026 18:37

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds a flaw in Cisco FMC and Cisco SCC Firewall Management to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a flaw in Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management, tracked as CVE-2026-20131 (CVSS score [...]

DarkSword emerges as powerful iOS exploit tool in global attacks

Security Affairs - 19 March 2026 15:03

DarkSword, a new iOS exploit kit, is used by multiple actors to steal data in campaigns targeting Saudi Arabia, Turkey, Malaysia, and Ukraine. Lookout Threat Labs discovered a new iOS exploit kit called DarkSword that has been used since late 2025 by multiple threat actors, including surveillance vendors and likely nation-state actors.

Apple Warns Older iPhones Vulnerable to Coruna, DarkSword Exploit Kit Attacks

The Hacker News - 20 March 2026 11:46

Apple is urging users who are still running an outdated version of iOS to update their iPhones to secure against web-based attacks carried out via powerful exploit kits like Coruna and DarkSword.

Scottish Cyber Coordination Centre

ThreatsDay Bulletin: FortiGate RaaS, Citrix Exploits, MCP Abuse, LiveChat Phish & More

The Hacker News - 19 March 2026 20:55

CISA Warns of Zimbra, SharePoint Flaw Exploits; Cisco Zero-Day Hit in Ransomware Attacks

The Hacker News - 19 March 2026 12:35

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has urged government agencies to apply patches for two security flaws impacting Synacor Zimbra Collaboration Suite (ZCS) and Microsoft Office SharePoint, stating they have been actively exploited in the wild.

Threat actors and malware

FBI seizes Handala data leak site after Stryker cyberattack

BleepingComputer - 19 March 2026 13:14

The FBI has seized two websites used by the Handala hacktivist group after the threat actors conducted a destructive cyberattack on medical technology giant Stryker that wiped approximately 80,000 devices. [...]

DoJ Disrupts 3 Million-Device IoT Botnets Behind Record 31.4 Tbps Global DDoS Attacks

The Hacker News - 20 March 2026 12:55

The U.S. Department of Justice (DoJ) on Thursday announced the disruption of command-and-control (C2) infrastructure used by several Internet of Things (IoT) botnets like AISURU, Kimwolf, JackSkid, and Mossad as part of a court-authorized law enforcement operation.

Speagle Malware Hijacks Cobra DocGuard to Steal Data via Compromised Servers

The Hacker News - 20 March 2026 01:46

Cybersecurity researchers have flagged a new malware dubbed Speagle that hijacks the functionality and infrastructure of a legitimate program called Cobra DocGuard."Speagle is designed to surreptitiously harvest sensitive information from infected computers and transmit it to a Cobra DocGuard server that has been compromised by the attackers, masking the data exfiltration process as legitimate

New Perseus Android Banking Malware Monitors Notes Apps to Extract Sensitive Data

The Hacker News - 19 March 2026 19:13

Cybersecurity researchers have disclosed a new Android malware family called Perseus that's being actively distributed in the wild with an aim to conduct device takeover (DTO) and financial fraud.Perseus is built upon the foundations of Cerberus and Phoenix, at the same time evolving into a "more flexible and capable platform" for compromising Android devices through dropper apps distributed

Scottish Cyber Coordination Centre

Iran Readied Cyberattack Capabilities for Response Prior to Epic Fury

SecurityWeek - 19 March 2026 16:30

Analysis reveals a six-month buildup of Iran-linked cyber infrastructure, including US-based shell companies, designed to weather kinetic strikes and ensure the resilience of its global hacking operations.

UK related

UK: Regulation Drives Cyber Spending for Critical Infrastructure Orgs

Infosecurity Magazine - 19 March 2026 10:00

35% of security leaders working in the UK's critical infrastructure said regulatory requirements are the primary influence on their security programs