Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 March 2026

Vulnerabilities

Attackers exploit FortiGate devices to access sensitive network information

Security Affairs - 10 March 2026 20:02

SentinelOne researchers warn that attackers are exploiting vulnerabilities or weak credentials in FortiGate devices to gain initial access to corporate networks. Once inside, they extract configuration files that may contain service account credentials and information about the internal network structure.

Microsoft March 2026 Patch Tuesday fixes 2 zero-days, 79 flaws

BleepingComputer - 10 March 2026 14:49

Today is Microsoft's March 2026 Patch Tuesday with security updates for 79 flaws, including 2 publicly disclosed zero-day vulnerabilities.

HPE warns of critical AOS-CX flaw allowing admin password resets

BleepingComputer - 10 March 2026 14:30

Hewlett Packard Enterprise (HPE) has patched multiple security vulnerabilities in the Aruba Networking AOS-CX operating system, including several authentication and code execution issues.

New "LeakyLooker" Flaws in Google Looker Studio Could Enable Cross-Tenant SQL Queries

The Hacker News - 10 March 2026 19:50

Cybersecurity researchers have disclosed nine cross-tenant vulnerabilities in Google Looker Studio that could have permitted attackers to run arbitrary SQL queries on victims' databases and exfiltrate sensitive data within organizations' Google Cloud environments.

Adobe Patches 80 Vulnerabilities Across Eight Products

SecurityWeek - 10 March 2026 19:22

Adobe has rolled out patches for 80 vulnerabilities across 8 products, including Commerce, Illustrator, Acrobat Reader, and Premiere Pro.

SAP Patches Critical FS-QUO, NetWeaver Vulnerabilities

SecurityWeek - 10 March 2026 15:31

A code injection bug in FS-QUO and an insecure deserialization flaw in NetWeaver could lead to arbitrary code execution.

Threat actors and malware

New ‘Zombie ZIP’ technique lets malware slip past security tools

BleepingComputer - 10 March 2026 17:05

A new technique dubbed “Zombie ZIP” helps conceal payloads in compressed files specially created to avoid detection from security solutions such as antivirus and endpoint detection and response (EDR) products.

‘BlackSanta’ EDR Killer Targets HR Workflows

darkreading - 10 March 2026 14:30

A campaign by Russian-speaking cyberattackers hijacks workflows to deliver security-busting malware, allowing attackers to steal data without detection.

New BeatBanker Android malware poses as Starlink app to hijack devices

BleepingComputer - 10 March 2026 18:27

A new Android malware named BeatBanker can hijack devices and tricks users into installing it by posing as a Starlink app on websites masquerading as the official Google Play Store.

Threat actors use custom AuraInspector to harvest data from Salesforce systems

Security Affairs - 10 March 2026 13:29

Salesforce CSOC warns that threat actors are mass-scanning publicly accessible Experience Cloud sites using a modified version of the AuraInspector tool. AuraInspector is an open-source command-line tool released by Google/Mandiant to audit Salesforce Aura and Experience Cloud.

APT28 Uses BEARDSHELL and COVENANT Malware to Spy on Ukrainian Military

The Hacker News - 10 March 2026 17:25

The Russian state-sponsored hacking group tracked as APT28 has been observed using a pair of implants dubbed BEARDSHELL and COVENANT to facilitate long-term surveillance of Ukrainian military personnel.

KadNap Malware Infects 14,000+ Edge Devices to Power Stealth Proxy Botnet

The Hacker News - 10 March 2026 22:30

Cybersecurity researchers have discovered a new malware called KadNap that’s primarily targeting Asus routers to enlist them into a botnet for proxying malicious traffic. The malware, first detected in the wild in August 2025, has expanded to over 14,000 infected devices, with more than 60% of victims located in the U.S.