Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 March 2026

Vulnerabilities

U.S. CISA adds Microsoft SharePoint and Zimbra flaws to its Known Exploited Vulnerabilities catalog

Security Affairs - 18 March 2026 22:11

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added SharePoint and Zimbra flaws to its Known Exploited Vulnerabilities (KEV) catalog. Below are the flaws added to the catalog:
CVE-2026-20963 (CVSS score of 8.8) – Microsoft SharePoint Deserialization of Untrusted Data Vulnerability
CVE-2025-66376 (CVSS score of 7.2) – Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability;

Interlock Ransomware Exploits Cisco FMC Zero-Day CVE-2026-20131 for Root Access

The Hacker News - 18 March 2026 22:30

The vulnerability in question is CVE-2026-20131 (CVSS score: 10.0), a case of insecure deserialization of user-supplied Java byte stream, which could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary Java code as root on an affected device.

'DarkSword' iOS Exploit Kit Used by State-Sponsored Hackers, Spyware Vendors

SecurityWeek - 18 March 2026 16:30

Targeting six iOS vulnerabilities and leading to full device compromise, the exploit chain is meant for surveillance.

ConnectWise patches new flaw allowing ScreenConnect hijacking

BleepingComputer - 18 March 2026 15:10

ConnectWise is warning ScreenConnect customers of a cryptographic signature verification vulnerability that could lead to unauthorized access and privilege escalation.

Ubuntu CVE-2026-3888 Bug Lets Attackers Gain Root via systemd Cleanup Timing Exploit

The Hacker News - 18 March 2026 14:38

A high-severity security flaw affecting default installations of Ubuntu Desktop versions 24.04 and later could be exploited to escalate privileges to the root level. Tracked as CVE-2026-3888 (CVSS score: 7.8), the issue could allow an attacker to seize control of a susceptible system.

Scottish Cyber Coordination Centre

Researchers warn of unpatched, critical Telnetd flaw affecting all versions

Security Affairs - 18 March 2026 16:06

Cybersecurity company Dream disclosed a critical flaw, tracked as CVE-2026-32746 (CVSS score of 9.8), in GNU InetUtils telnetd that lets unauthenticated remote attackers execute code with elevated privileges.

Threat actors and malware

Iranian Hackers Likely Used Malware-Stolen Credentials in Stryker Breach

SecurityWeek - 18 March 2026 13:47

The medtech giant has been working on restoring systems affected by the cyberattack conducted by the Handala hackers.

Vidar Stealer 2.0 Exploits GitHub, Reddit to Deliver Malware via Fake Game Cheats

Infosecurity Magazine - 18 March 2026 12:15

The Vidar 2.0 infostealers is deployed through fake free game cheats on GitHub and Reddit