Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 March 2025

Vulnerabilities

Ongoing Cyber Attacks Exploit Critical Vulnerabilities in Cisco Smart Licensing Utility

The Hacker News - 21 March 2025 11:39

Two now-patched security flaws impacting Cisco Smart Licensing Utility are seeing active exploitation attempts, according to SANS Internet Storm Center. The two critical-rated vulnerabilities in question are listed below - CVE-2024-20439 (CVSS score: 9.8) and CVE-2024-20440 (CVSS score: 9.8).

CISA Warns of Exploited Nakivo Vulnerability

SecurityWeek - 20 March 2025 16:30

CISA has added an absolute path traversal bug in Nakivo Backup and Replication to its Known Exploited Vulnerabilities list.

Veeam fixed critical Backup & Replication flaw CVE-2025-23120

Security Affairs - 20 March 2025 20:26

Veeam addressed a critical security vulnerability, tracked as CVE-2025-23120 (CVSS score of 9.9), impacting its Backup & Replication software that could lead to remote code execution. The vulnerability impacts 12.3.0.310 and all earlier version 12 builds.

WordPress security plugin WP Ghost vulnerable to remote code execution bug

BleepingComputer - 20 March 2025 11:58

Popular WordPress security plugin WP Ghost is vulnerable to a critical severity flaw that could allow unauthenticated attackers to remotely execute code and hijack servers.

Threat actors and malware

VSCode extensions found downloading early-stage ransomware

BleepingComputer - 20 March 2025 16:54

Two malicious VSCode Marketplace extensions were found deploying in-development ransomware from a remote server, exposing critical gaps in Microsoft's review process.

Scottish Cyber Coordination Centre

UK urges critical orgs to adopt quantum cryptography by 2035

BleepingComputer - 20 March 2025 13:23

The UK's National Cyber Security Centre (NCSC) has published specific timelines on migrating to post-quantum cryptography (PQC), dictating that critical organizations should complete migration by 2035.

RansomHub ransomware uses new Betruger 'multi-function' backdoor

BleepingComputer - 20 March 2025 13:31

Security researchers have linked a new backdoor dubbed Betruger, deployed in several recent ransomware attacks, to an affiliate of the RansomHub operation.

HellCat hackers go on a worldwide Jira hacking spree

BleepingComputer - 20 March 2025 10:44

Swiss global solutions provider Ascom has confirmed a cyberattack on its IT infrastructure as a hacker group known as Hellcat targets Jira servers worldwide using compromised credentials.

VexTrio Using 20,000 Hacked WordPress Sites in Traffic Redirect Scheme

darkreading - 20 March 2025 21:05

A massive cybercrime network known as "VexTrio" is using thousands of compromised WordPress sites to funnel traffic through a complex redirection scheme.