Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 April 2025

Vulnerabilities

CISA Warns of CrushFTP Vulnerability Exploitation in the Wild

Infosecurity Magazine - 08 April 2025 12:20

The US Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2025-31161 to its Known Exploited Vulnerabilities (KEV) catalog.

Microsoft April 2025 Patch Tuesday fixes exploited zero-day, 134 flaws

BleepingComputer - 08 April 2025 14:50

Today is Microsoft's April 2025 Patch Tuesday, which includes security updates for 134 flaws, including one actively exploited zero-day vulnerability.

Adobe Patches 11 Critical ColdFusion Flaws Amid 30 Total Vulnerabilities Discovered

The Hacker News - 09 April 2025 09:42

Adobe has released security updates to fix a fresh set of security flaws, including multiple critical-severity bugs in ColdFusion versions 2025, 2023 and 2021 that could result in arbitrary file read and code execution. Of the 30 flaws in the product, 11 are rated Critical in severity.

SAP Patches Critical Code Injection Vulnerabilities

SecurityWeek - 08 April 2025 14:22

SAP released 20 security notes on April 2025 patch day, including three addressing critical code injection and authentication bypass flaws.

Fortinet Urges FortiSwitch Upgrades to Patch Critical Admin Password Change Flaw

The Hacker News - 09 April 2025 00:23

Fortinet has released security updates to address a critical security flaw impacting FortiSwitch that could permit an attacker to make unauthorized password changes. The vulnerability, tracked as CVE-2024-48887, carries a CVSS score of 9.3 out of a maximum of 10.0.

Amazon EC2 SSM Agent Flaw Patched After Privilege Escalation via Path Traversal

The Hacker News - 08 April 2025 23:26

Cybersecurity researchers have disclosed details of a now-patched security flaw in the Amazon EC2 Simple Systems Manager (SSM) Agent that, if successfully exploited, could permit an attacker to achieve privilege escalation and code execution.

WhatsApp fixed a spoofing flaw that could enable Remote Code Execution

Security Affairs - 08 April 2025 15:25

WhatsApp released a security update to address a vulnerability, tracked as CVE-2025-30401, that could let attackers trick users and enable remote code execution.

Threat actors and malware

Fake Microsoft Office add-in tools push malware via SourceForge

BleepingComputer - 08 April 2025 17:53

Threat actors are abusing SourceForge to distribute fake Microsoft add-ins that install malware on victims' computers to both mine and steal cryptocurrency.

AWS rolls out ML-KEM to secure TLS from quantum threats

BleepingComputer - 08 April 2025 11:54

Amazon Web Services (AWS) has added support for the ML-KEM post-quantum key encapsulation mechanism to AWS Key Management Service (KMS), AWS Certificate Manager (ACM), and AWS Secrets Manager, making TLS connections more secure.

UAC-0226 Deploys GIFTEDCROOK Stealer via Malicious Excel Files Targeting Ukraine

The Hacker News - 08 April 2025 16:42

The Computer Emergency Response Team of Ukraine (CERT-UA) has revealed a new set of cyber attacks targeting Ukrainian institutions with information-stealing malware. The activity is aimed at military formations, law enforcement agencies, and local self-government bodies, particularly those located near Ukraine's eastern border, the agency said.