Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 March 2025

Vulnerabilities

CISA Urges All Organizations to Patch Exploited Critical Ivanti Vulnerabilities

Infosecurity Magazine - 11 March 2025 13:00

The US Cybersecurity and Infrastructure Security Agency (CISA) has added five new flaws in Ivanti and VeraCore products to its Known Exploited Vulnerabilities catalog

CISA Adds Six Known Exploited Vulnerabilities to Catalog

CISA Advisories – 11 March 2025

CISA has added six new vulnerabilities to its Known Exploited Vulnerabilities Catalog,

- CVE-2025-24983 Microsoft Windows Win32k Use-After-Free Vulnerability
- CVE-2025-24984 Microsoft Windows NTFS Information Disclosure Vulnerability
- CVE-2025-24985 Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability
- CVE-2025-24991 Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability
- CVE-2025-24993 Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability
- CVE-2025-26633 Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability

Apple fixed the third actively exploited zero-day of 2025

Security Affairs - 11 March 2025 23:48

Apple has released emergency security updates to address a zero-day vulnerability, tracked as CVE-2025-24201, in the WebKit cross-platform web browser engine. The vulnerability is an out-of-bounds write issue that was exploited in “extremely sophisticated” attacks.

Patch Tuesday: Critical Code Execution Bugs in Adobe Acrobat and Reader

SecurityWeek - 11 March 2025 18:33

Adobe documents 35 security flaws in a wide range of products, including code-execution issues in the Acrobat and Reader applications.

Microsoft March 2025 Patch Tuesday fixes 7 zero-days, 57 flaws

BleepingComputer - 11 March 2025 14:45

Today is Microsoft’s March 2025 Patch Tuesday, which includes security updates for 57 flaws, including six actively exploited zero-day vulnerabilities.

Scottish Cyber Coordination Centre

SAP Patches High-Severity Vulnerabilities in Commerce, NetWeaver

SecurityWeek - 11 March 2025 13:57

SAP released 21 new security notes and updated three security notes on March 2025 security patch day.

Moxa Issues Fix for Critical Authentication Bypass Vulnerability in PT Switches

The Hacker News - 11 March 2025 13:15

Taiwanese company Moxa has released a security update to address a critical security flaw impacting its PT switches that could permit an attacker to bypass authentication guarantees. The vulnerability, tracked as CVE-2024-12297, has been assigned a CVSS v4 score of 9.2 out of a maximum of 10.0.

Threat actors and malware

North Korean Lazarus hackers infect hundreds via npm packages

BleepingComputer - 11 March 2025 17:42

Six malicious packages have been identified on npm (Node package manager) linked to the notorious North Korean hacking group Lazarus.

Ballista Botnet Exploits Unpatched TP-Link Vulnerability, Targets Over 6,000 Devices

The Hacker News - 11 March 2025 19:00

Unpatched TP-Link Archer routers have become the target of a new botnet campaign dubbed Ballista, according to new findings from the Cato CTRL team. The botnet exploits a remote code execution (RCE) vulnerability in TP-Link Archer routers (CVE-2023-1389) to spread itself automatically over the Internet.