Scottish Cyber Coordination Centre

Daily Threat Bulletin

4 March 2025

Vulnerabilities

Microsoft links recent Microsoft 365 outage to buggy update

BleepingComputer - 03 March 2025 10:37

Microsoft says a coding issue is behind a now-resolved Microsoft 365 outage over the weekend that affected Outlook and Exchange Online authentication. [...]

Cisco, Hitachi, Microsoft, and Progress Flaws Actively Exploited—CISA Sounds Alarm

The Hacker News - 04 March 2025 11:09

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added five security flaws impacting software from Cisco, Hitachi Vantara, Microsoft Windows, and Progress WhatsUp Gold to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.

Google's March 2025 Android Security Update Fixes Two Actively Exploited Vulnerabilities

The Hacker News - 04 March 2025 10:37

Google has released its monthly Android Security Bulletin for March 2025 to address a total of 44 vulnerabilities, including two that it said have come under active exploitation in the wild.

CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added five new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2023-20118 Cisco Small Business RV Series Routers Command Injection VulnerabilityCVE-2022-43939 Hitachi Vantara Pentaho BA Server Authorization Bypass VulnerabilityCVE-2022-43769 Hitachi Vantara Pentaho BA Server Special Element Injection VulnerabilityCVE-2018-8639 Microsoft Windows Win32k Improper Resource Shutdown or Release VulnerabilityCVE-2024-4885 Progress WhatsUp Gold Path Traversal Vulnerability.

Threat actors and malware

DHS says CISA will not stop monitoring Russian cyber threats

BleepingComputer - 03 March 2025 15:22

The US Cybersecurity and Infrastructure Security Agency says that media reports about it being directed to no longer follow or report on Russian cyber activity are untrue, and its mission remains unchanged. [...]

Scottish Cyber Coordination Centre

New ClickFix attack deploys Havoc C2 via Microsoft Sharepoint

BleepingComputer - 03 March 2025 13:33

A newly uncovered ClickFix phishing campaign is tricking victims into executing malicious PowerShell commands that deploy the Havok post-exploitation framework for remote access to compromised devices. [...]

Hackers Exploit AWS Misconfigurations to Launch Phishing Attacks via SES and WorkMail

The Hacker News - 03 March 2025 23:56

Threat actors are targeting Amazon Web Services (AWS) environments to push out phishing campaigns to unsuspecting targets, according to findings from Palo Alto Networks Unit 42.

Hackers Use ClickFix Trick to Deploy PowerShell-Based Havoc C2 via SharePoint Sites

The Hacker News - 03 March 2025 20:30

Cybersecurity researchers are calling attention to a new phishing campaign that employs the ClickFix technique to deliver an open-source command-and-control (C2) framework called Havoc.

Vulnerable Paragon Driver Exploited in Ransomware Attacks

SecurityWeek - 03 March 2025 12:58

Ransomware operators exploit a vulnerable Paragon driver in BYOVD attacks to elevate privileges to System.