Scottish Cyber Coordination Centre

Daily threat bulletin

7 February 2025

Vulnerabilities

Critical RCE bug in Microsoft Outlook now exploited in attacks

BleepingComputer - 06 February 2025 14:17

CISA warned U.S. federal agencies on Thursday to secure their systems against ongoing attacks targeting a critical Microsoft Outlook remote code execution (RCE) vulnerability. [...]

Hackers Exploiting SimpleHelp RMM Flaws for Persistent Access and Ransomware

The Hacker News - 07 February 2025 11:49

Threat actors have been observed exploiting recently disclosed security flaws in SimpleHelp's Remote Monitoring and Management (RMM) software as a precursor for what appears to be a ransomware attack.

CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added five vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2025-0411 7-Zip Mark of the Web Bypass VulnerabilityCVE-2022-23748 Dante Discovery Process Control VulnerabilityCVE-2024-21413 Microsoft Outlook Improper Input Validation VulnerabilityCVE-2020-29574 CyberoamOS (CROS) SQL Injection VulnerabilityCVE-2020-15069 Sophos XG Firewall Buffer Overflow Vulnerability

Cisco addressed two critical flaws in its Identity Services Engine (ISE)

Security Affairs - 06 February 2025 16:42

Cisco addressed critical flaws in Identity Services Engine, preventing privilege escalation and system configuration changes. Cisco addressed multiple vulnerabilities, including two critical remote code execution flaws, tracked as CVE-2025-20124 (CVSS score of 9.9) and CVE-2025-20125 (CVSS score of 9.1), in Identity Services Engine (ISE).

WordPress ASE Plugin Vulnerability Threatens Site Security

Infosecurity Magazine - 06 February 2025 17:30

Patchstack urges admins to patch new WordPress ASE plugin vulnerability that lets users restore previous admin privileges

Threat actors and malware

North Korean APT Kimsuky Uses forceCopy Malware to Steal Browser-Stored Credentials

The Hacker News - 06 February 2025 17:35

The North Korea-linked nation-state hacking group known as Kimsuky has been observed conducting spear-phishing attacks to deliver an information stealer malware named forceCopy, according to new findings from the AhnLab Security Intelligence Center (ASEC).

Microsoft says attackers use exposed ASP.NET keys to deploy malware

BleepingComputer - 06 February 2025 16:59

Microsoft warns that attackers are deploying malware in ViewState code injection attacks using static ASP. NET machine keys found online. [...]

Fake Google Chrome Sites Distribute ValleyRAT Malware via DLL Hijacking

The Hacker News - 06 February 2025 21:04

Bogus websites advertising Google Chrome have been used to distribute malicious installers for a remote access trojan called ValleyRAT.The malware, first detected in 2023, is attributed to a threat actor tracked as Silver Fox, with prior attack campaigns primarily targeting Chinese-speaking regions like Hong Kong, Taiwan, and Mainland China.

Apple missed screenshot-snooping malware in code that made it into the App Store, Kaspersky claims

The Register - 07 February 2025 04:03

OCR plugin great for extracting crypto-wallet secrets from galleries Kaspersky eggheads say they've spotted the first app containing hidden optical character recognition spyware in Apple's App Store.

UK related

British engineering firm IMI discloses breach, shares no details

BleepingComputer - 06 February 2025 10:36

British-based engineering firm IMI plc has disclosed a security breach after unknown attackers hacked into the company's systems. [...]

New UK Cyber Monitoring Centre Introduces 'Richter Scale' for Cyber-Attacks

Infosecurity Magazine - 06 February 2025 16:10

This new independent non-profit was set up by the UK insurance industry to bring more transparency around cyber events