Scottish Cyber Coordination Centre

Daily threat bulletin

13 February 2025

Vulnerabilities

Researchers Find New Exploit Bypassing Patched NVIDIA Container Toolkit Vulnerability

The Hacker News - 12 February 2025 20:34

Cybersecurity researchers have discovered a bypass for a now-patched security vulnerability in the NVIDIA Container Toolkit that could be exploited to break out of a container's isolation protections and gain complete access to the underlying host.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2025-24200 Apple iOS and iPadOS Incorrect Authorization Vulnerability; CVE-2024-41710 Mitel SIP Phones Argument Injection Vulnerability.

Surge in attacks exploiting old ThinkPHP and ownCloud flaws

BleepingComputer - 12 February 2025 19:04

Increased hacker activity has been observed in attempts to compromise poorly maintained devices that are vulnerable to older security issues from 2022 and 2023. [...]

Threat actors and malware

Russian Seashell Blizzard Hackers Have Access to Critical Infrastructure: Microsoft

SecurityWeek - 12 February 2025 18:01

A subgroup of the Russia-linked Seashell Blizzard is tasked with broad initial access operations to sustain long-term persistence.

North Korea-linked APT Emerald Sleet is using a new tactic

Security Affairs - 12 February 2025 12:55

Microsoft Threat Intelligence has observed North Korea-linked APT Emerald Sleet using a new tactic, tricking targets into running PowerShell. Microsoft Threat Intelligence researchers spotted North Korea-linked threat actor Emerald Sleet (also known as Kimsuky and VELVET CHOLLIMA) using a new tactic.

Lines Between Nation-State and Cybercrime Groups Disappearing: Google

Security Boulevard - 13 February 2025 06:11

Threat researchers with Google are saying that the lines between nation-state actors and cybercrime groups are blurring, noting that gangs backed by China, Russia, and others are using financially motivated hackers and their tools while attacks by cybercriminals should be seen as national security threats.

US, UK and Australia Sanction Russian Bulletproof Hoster Zservers

Infosecurity Magazine - 12 February 2025 10:30

The US and its allies have sanctioned Russian bulletproof hoster Zservers for abetting ransomware attacks