Scottish Cyber Coordination Centre

Daily Threat Bulletin

7 March 2025

Vulnerabilities

Over 37,000 VMware ESXi servers vulnerable to ongoing attacks

BleepingComputer - 06 March 2025 11:39

Over 37,000 internet-exposed VMware ESXi instances are vulnerable to CVE-2025-22224, a critical out-of-bounds write flaw that is actively exploited in the wild. [...]

PHP-CGI RCE Flaw Exploited in Attacks on Japan's Tech, Telecom, and E-Commerce Sectors

The Hacker News - 07 March 2025 11:12

Threat actors of unknown provenance have been attributed to a malicious campaign predominantly targeting organizations in Japan since January 2025."The attacker has exploited the vulnerability CVE-2024-4577, a remote code execution (RCE) flaw in the PHP-CGI implementation of PHP on Windows, to gain initial access to victim machines.

Elastic Releases Urgent Fix for Critical Kibana Vulnerability Enabling Remote Code Execution

The Hacker News - 06 March 2025 19:03

Elastic has rolled out security updates to address a critical security flaw impacting the Kibana data visualization dashboard software for Elasticsearch that could result in arbitrary code execution. The vulnerability, tracked as CVE-2025-25012, carries a CVSS score of 9.9 out of a maximum of 10.0. It has been described as a case of prototype pollution.

House Passes Bill Requiring Federal Contractors to Implement Vulnerability Disclosure Policies

SecurityWeek - 06 March 2025 14:50

The House of Representatives has passed a bill aimed at requiring federal contractors to have a Vulnerability Disclosure Policy (VDP).

Threat actors and malware

Microsoft says malvertising campaign impacted 1 million PCs

BleepingComputer - 06 March 2025 16:53

Microsoft has taken down an undisclosed number of GitHub repositories used in a massive malvertising campaign that impacted almost one million devices worldwide. [...]

Malicious Chrome extensions can spoof password managers in new attack

BleepingComputer - 06 March 2025 10:19

A newly devised “polymorphic” attack allows malicious Chrome extensions to morph into other browser extensions, including password managers, crypto wallets, and banking apps, to steal sensitive information. [...]

EncryptHub Deploys Ransomware and Stealer via Trojanized Apps, PPI Services, and Phishing

The Hacker News - 06 March 2025 18:45

The financially motivated threat actor known as EncryptHub has been observed orchestrating sophisticated phishing campaigns to deploy information stealers and ransomware, while also working on a new product called EncryptRAT.

Medusa Ransomware Hits 40+ Victims in 2025, Demands $100K–$15M Ransom

The Hacker News - 06 March 2025 18:31

The threat actors behind the Medusa ransomware have claimed nearly 400 victims since it first emerged in January 2023, with the financially motivated attacks witnessing a 42% increase between 2023 and 2024.

Over 1,000 WordPress Sites Infected with JavaScript Backdoors Enabling Persistent Attacker Access

The Hacker News - 06 March 2025 16:27

Over 1,000 websites powered by WordPress have been infected with a third-party JavaScript code that injects four separate backdoors.”Creating four backdoors facilitates the attackers having multiple points of re-entry should one be detected and removed,” c/side researcher Himanshu Anand said in a Wednesday analysis.