Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

11 March 2025

Vulnerabilities

Experts warn of mass exploitation of critical PHP flaw CVE-2024-4577

Security Affairs - 10 March 2025 15:52

Threat actors exploit PHP flaw CVE-2024-4577 for remote code execution. Over 1,000 attacks detected globally. GreyNoise researchers warn of a large-scale exploitation of a critical vulnerability, tracked as CVE-2024-4577 (CVSS 9.8), in PHP. An attacker could exploit the vulnerability to achieve remote code execution on vulnerable servers using Apache and PHP-CGI. The flaw CVE-2024-4577 (CVSS score: 9.8) is […]

Details Disclosed for SCADA Flaws That Could Facilitate Industrial Attacks

SecurityWeek - 10 March 2025 18:01

Palo Alto Networks has shared details on several high-severity Mitsubishi Electric and Iconics SCADA vulnerabilities.

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-2025-25181 Advantive VeraCore SQL Injection Vulnerability; CVE-2024-57968 Advantive VeraCore Unrestricted File Upload Vulnerability; CVE-2024-13159 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability; CVE-2024-13160 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability; CVE-2024-13161 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability.

Threat actors and malware

X hit by ‘massive cyberattack’ amid Dark Storm’s DDoS claims

BleepingComputer - 10 March 2025 17:07

The Dark Storm hacktivist group claims to be behind DDoS attacks causing multiple X worldwide outages on Monday, leading the company to enable DDoS protections from Cloudflare. […]

Researchers Expose New Polymorphic Attack That Clones Browser Extensions to Steal Credentials

The Hacker News - 10 March 2025 21:17

Cybersecurity researchers have demonstrated a novel technique that allows a malicious web browser extension to impersonate any installed add-on.”The polymorphic extensions create a pixel perfect replica of the target’s icon, HTML popup, workflows and even temporarily disables the legitimate extension, making it extremely convincing for victims to believe that they are providing credentials to

GitHub-Hosted Malware Infects 1M Windows Users

darkreading - 10 March 2025 11:43

Microsoft has identified a complex, malvertising-based attack chain that delivered Lumma and other infostealers to enterprise and consumer PC users; the campaign is unlikely the last of its kind.

UK related

More than 90 NHS staff viewed attacks victims' data

BBC News - 10 March 2025 19:15

A hospital trust is investigating concerns some staff "inappropriately accessed" the records.