Scottish Cyber Coordination Centre

Daily threat bulletin

3 April 2024

Vulnerabilities

XSS flaw in WordPress WP-Members Plugin can lead to script injection

Security Affairs - 02 April 2024 19:59

A cross-site scripting vulnerability (XXS) in the WordPress WP-Members Membership plugin can lead to malicious script injection. Researchers from Defiant's Wordfence research team disclosed a cross-site scripting vulnerability (XXS) in the WordPress WP-Members Membership plugin that can lead to malicious script injection. The Unauthenticated Stored Cross-Site Scripting vulnerability was reported to Wordfence by the WordPress [...]

Malicious Code in XZ Utils for Linux Systems Enables Remote Code Execution

The Hacker News - 02 April 2024 19:48

The malicious code inserted into the open-source library XZ Utils, a widely used package present in major Linux distributions, is also capable of facilitating remote code execution, a new analysis has revealed.The audacious supply chain compromise, tracked as CVE-2024-3094 (CVSS score: 10.0), came to light last week when Microsoft engineer and PostgreSQL developer Andres Freund...

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2023-24955 Microsoft SharePoint Server Code Injection Vulnerability.

Rockwell Automation FactoryTalk View ME

CISA Advisories -

Rockwell FactoryTalk View ME - A vulnerability exists in the affected product that allows a malicious user to restart the PanelView Plus 7 terminal remotely without security protections. If the vulnerability is exploited, it could lead to the loss of view or control of the PanelView product. CVE-2024-21914 has been assigned to this vulnerability. A CVSS v3.1 base score of 5.3 has been calculated.

Scottish Cyber Coordination Centre

Threat actors and malware

Winnti's new UNAPIMON tool hides malware from security software

BleepingComputer - 02 April 2024 18:59

The Chinese 'Winnti' hacking group was found using a previously undocumented malware called UNAPIMON to let malicous processes run without being detected. [...]

Cyberattacks Wreaking Physical Disruption on the Rise

darkreading - 02 April 2024 13:00

Ransomware groups tore into manufacturing other parts of the OT sector in 2023, and a few attacks caused eight- and nine-figure damages. But worse is yet to come in 2024.

Microsoft slammed for lax security that led to China's cyber-raid on Exchange Online

The Register - 03 April 2024 03:15

CISA calls for 'fundamental, security-focused reforms' to happen ASAP, delaying work on other software A review of the June 2023 attack on Microsoft's Exchange Online hosted email service – which saw accounts used by senior US officials compromised by a China-linked group called "Storm-0558" – has found that the incident would have been preventable save for Microsoft's lax infosec culture and sub-par cloud security precautions....

INC Ransom claims to be behind 'cyber incident' at UK city council

The Register - 02 April 2024 12:15

This follows attack on NHS services in Scotland last week The cyber skids at INC Ransom are claiming responsbility for the ongoing cybersecurity incident at Leicester City Council, according to a post caught by eagle-eyed infosec watchers....