Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

23 February 2024

Vulnerabilities

Zero-Click Apple Shortcuts Vulnerability Allows Silent Data Theft

Dark Reading - February 22 2024

Vulnerability CVE-2024-23204, affecting Apple's popular Shortcuts app, suggests a critical need for ongoing security awareness in the macOS and iOS ecosystem.

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Answer[.]This issue [CVE-2024-23349]

nvd.nist.gov - February 22 2024

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Answer[.]This issue affects Apache Answer: through 1.2.1. XSS attack when user enters summary. A logged-in user, when modifying their own submitted question, can input malicious code in the summary to create such an attack. Users are recommended to upgrade to version [1.2.5], which fixes the issue.

Multiple XSS flaws in Joomla can lead to remote code execution

Security Affairs - February 22 2024

Joomla maintainers have addressed multiple vulnerabilities in the popular content management system (CMS) that can lead to execute arbitrary code.

Delta Electronics CNCSoft-B DOPSoft

CISA Current Activity - February 22 2024

EXECUTIVE SUMMARY CVSS v3 7.8 ATTENTION: Low attack complexity Vendor: Delta Electronics Equipment: CNCSoft-B DOPSoft Vulnerability: Uncontrolled Search Path Element 2. RISK EVALUATION Successful exploitation of this vulnerability could allow an attacker to achieve remote code execution.

Malware and threat actors

Ransomware associated with LockBit still spreading 2 days after server takedown

ArsTechnica - February 22 2024

Two days after an international team of authorities struck a major blow at LockBit, one of the Internet’s most prolific ransomware syndicates, researchers have detected a new round of attacks that are installing malware associated with the group.

TLP CLEAR: Disclosure is not limited

Russian Turla Cyberspies Target Polish NGOs With New Backdoor

SecurityWeek RSS Feed - February 22 2024

Russian state-sponsored threat actor Turla has been using a new backdoor in recent attacks targeting Polish NGOs. The post Russian Turla Cyberspies Target Polish NGOs With New Backdoor appeared first on SecurityWeek.