



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in SPIP CMS

Tracking #:432316276

Date:13-09-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability, designated as CVE-2024-8517, has been identified in the SPIP open-source content management system.

TECHNICAL DETAILS:

A critical security vulnerability, designated as CVE-2024-8517, has been identified in the SPIP open-source content management system. This vulnerability could allow unauthorized access and manipulation of sensitive data. A patch has been released to address this issue

- **CVE ID: CVE-2024-8517**- SPIP before 4.3.2, 4.2.16, and 4.1.18 is vulnerable to a command injection issue
- **Score:9.8 (Critical)**
- A remote and unauthenticated attacker can execute arbitrary operating system commands by sending a crafted multipart file upload HTTP request.
- **Affected Versions:** Versions prior to 4.3.2, 4.2.16, and 4.1.18.
- **Fixed Versions:** SPIP versions 4.3.2, 4.2.16, and 4.1.18.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update SPIP to the fixed version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://nvd.nist.gov/vuln/detail/CVE-2024-8517>