aDvens

Security for the greater good

Newscast
Vulnerability in Joomla

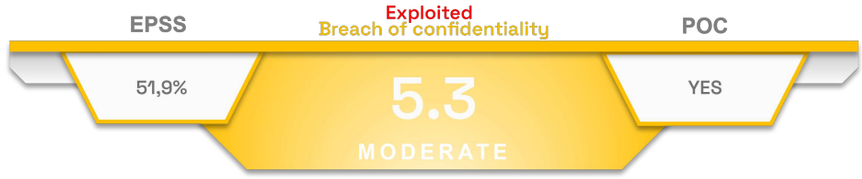
2024-01-10 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-23752

On 16 February 2023, Joomla published a security advisory concerning a vulnerability in its **Core**.



A security researcher from NSFOCUS TIANJI Lab has identified an access validation flaw in Joomla's web service endpoints in Joomla.

By sending a specifically crafted request, a remote and unauthenticated attacker can access confidental information from the web service.

This vulnerability is exploited since March 2023.
CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on 8 January 2024.

Type of vulnerability

- **CWE-284**: Improper Access Control

Risks

- Impact on data confidentiality

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	None	Impact on integrity	None
User Interaction	None	Impact on availability	None

Affected products

- Joomla! CMS versions 4.0.0 to 4.2.7

Recommendations

- Update to the version 4.2.8 ou later.
- Additional information is available in Joomla's advisory.

Proof of concept

A proof of concept is available in open source.

Sources

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23752
- https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2024/01/08/cisa-adds-six-known-exploited-vulnerabilities-catalog