

## Joomla! CMS Improper Access Check Vulnerability

**High target vulnerability leading to disclosure of sensitive information**

<https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html>  
 CVEs: CVE-2023-23752

An attack attempt to exploit an Improper Access Vulnerability in Joomla! CMS. The vulnerability is due to improper access control. Successful exploitation could lead to unauthorized access of sensitive information in the application. According to the vendor, the impact of exploitation of this flaw is critical.


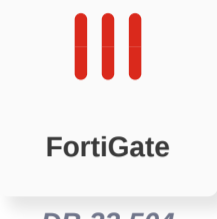

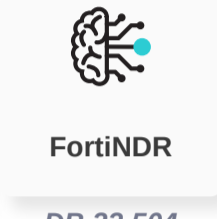
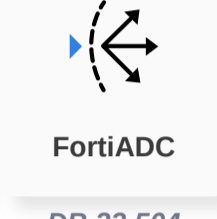

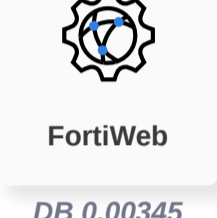

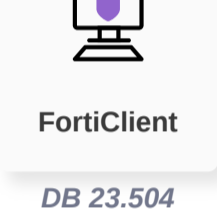
**Background** Joomla! is a free and open-source content management system (CMS) for publishing web content. Joomla's content management system, is developed using PHP language and MySQL database, and can run on various platforms such as Linux, Windows, and MacOSX. Joomla! CMS versions 4.0.0-4.2.7 is vulnerable to improper access check in webservice endpoints which may eventually leads to the disclosure of sensitive information such as account information, usernames or passwords.

**Announced** February 13, 2023: Issue was reported to Joomla! by Zewei Zhang from NSFOCUS TIANJI Lab.  
 February 16, 2023: Version 4.2.8 released by the Vendor which provided fix for CVE-2023-23752.

**Latest Developments** March 9, 2023: FortiGuard labs is seeing high IPS detections since a public exploit code is released and recommends admins to update the vulnerable Joomla! versions to 4.2.8 or above.  
<https://downloads.joomla.org/>

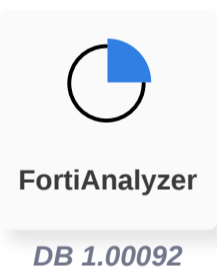
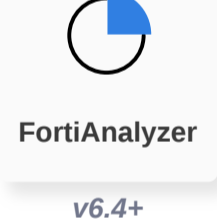

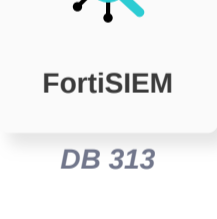
### PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance**
  - Decoy VM**  
 Deploys decoys across the network segments to detect activities related to the Improper Access Vulnerability in Joomla! CMS (CVE-2023-23752)  

- Weaponization**
- Delivery**
- Exploitation**
  - IPS**  
 Detects and blocks Improper Access Vulnerability in Joomla! CMS (CVE-2023-23752)  





  - Web App Security**  
 Detects and blocks Improper Access Vulnerability in Joomla! CMS (CVE-2023-23752)  


  - Application Firewall**  
 Detects and blocks Improper Access Vulnerability in Joomla! CMS (CVE-2023-23752)  

- Installation**
- C2**
- Action**

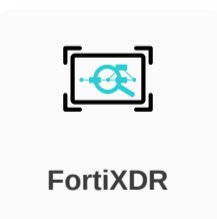
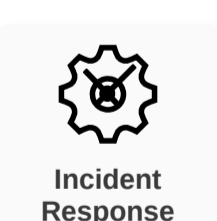
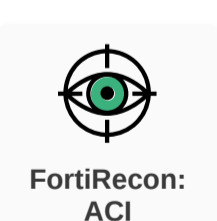
### DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

- Outbreak Detection**  

- Threat Hunting**  


- Content Update**  


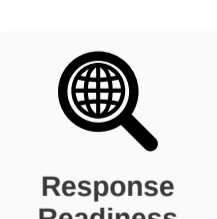
### RESPOND

Develop containment techniques to mitigate impacts of security events:

- Automated Response**  
 Services that can automatically respond to this outbreak.  

- Assisted Response Services**  
 Experts to assist you with analysis, containment and response activities.  



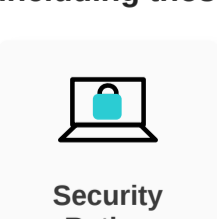
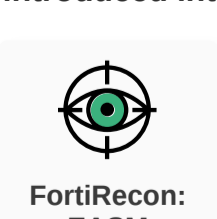
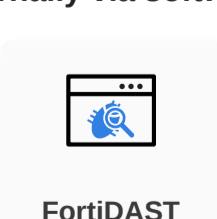
### RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

- InfoSec Services**  
 Security readiness and awareness training for SOC teams, InfoSec and general employees.  


### IDENTIFY

Identify processes and assets that need protection:

- Attack Surface Monitoring (Inside & Outside)**  
 Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.  




## Additional Resources

Joomla Security Centre <https://developer.joomla.org/security-centre.html>

Learn more about [FortiGuard Outbreak Alerts](#)