



PROFILE

CVE-2023-23752

ZEROFOX INTELLIGENCE

P-2023-04-05a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Common Vulnerabilities & Exposures

April 5, 2023



PROFILE: CVE-2023-23752

P-2023-04-05a

TLP:CLEAR

Created on: April 3, 2023

Intelligence Cut-off: 12:00 PM (DST) on April 4, 2023

First Observed: January 5, 2023

CVE Dictionary Entry: CVE-2022-44877

NVD Published Date: February 16, 2023

NVD Last Modified: February 24, 2023

Severity: MEDIUM

Base Score: 5.3

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Metasploit Available: No

Current Description

An issue was discovered in Joomla 4.0.0 through 4.2.7. An improper access check allows unauthorized access to web service endpoints.

Risk

CVE-2023-23752 is an information disclosure vulnerability that allows a threat actor unauthenticated access to sensitive APIs. The likelihood of a threat actor leveraging this vulnerability to scan for and exploit APIs is High, as the overhead associated with making a script to send simple HTTP requests is so extremely low.

CVE-2023-23752 allows threat actors to leak sensitive information associated with Joomla users, such as usernames and permissions. This vulnerability also allows the threat actor to obtain MySQL account login credentials Joomla uses to query a database. ZeroFox assesses that the overall impact is Medium but can quickly escalate to High if the MySQL database is exposed to the open internet.

ZeroFox assesses that the overall risk associated with CVE-2023-23752 is High due to the likelihood of exploitation, although the impact of successful exploitation is a Medium risk.

Known Affected Software Configurations

Configuration	Common Platform Enumeration
1	cpe:2.3:a:joomla:joomla\ :*****



Weakness Enumeration

CWE-ID	CWE Name	Source
NVD-CWE-Other	other	NIST

Summary

CVE-2023-23752 is an unauthenticated information disclosure within Joomla 4.0.0 <= and <= 4.2.7, which was disclosed on February 2, 2023, and patched on February 16, 2023.

The simplicity of this exploit allows threat actors to scan for this vulnerability easily. Even after a patch has been released for this vulnerability, threat actors are still looking for vulnerable systems. This active interest is shown in Figure 1 below; GreyNoise[.]io detected 21 unique IP addresses attempting to exploit CVE-2023-23752 throughout the month of March 2023.



Figure 1. Unique IP Scanning for CVE-2023-23752 Over Time

Source: [hXXps://viz.greynoise\[.\]io/tag/joomla-credential-disclosure-cve-2023-23752-attempt?days=30](https://viz.greynoise[.]io/tag/joomla-credential-disclosure-cve-2023-23752-attempt?days=30)

This vulnerability allows for a multitude of endpoints within Joomla to be publicly accessible, but the two main endpoints of interest for threat actors are */v1/config/application* and */v1/users*. More specifically, */v1/users* allows for the leak of usernames and privileges within a vulnerable Joomla instance, while the endpoint



/v1/config/application allows for the leak of MySQL credentials used by the Joomla instance.

If the MySQL port is exposed to the internet, then this information disclosure vulnerability can escalate to a Remote Code Execution vulnerability by manually changing the Joomla superuser account password within the database. The threat actor can then use the functionality of a super user account to execute arbitrary system commands.

Recommendation

A patch for CVE-2023-23752 was released on February 16, 2023; ZeroFox recommends updating to the latest version. If updating is not immediately possible, put this application behind a VPN, limiting its exposure to the internet. ZeroFox also recommends installing and configuring Filebeat to ingest logs. Finally, ZeroFox recommends blocking MySQL from being accessible via the internet if possible.



Appendix 1: Indicators of Compromise (Sigma Rules)

```
title: CVE-2023-23752
id: 28bb0c02-5440-4790-a696-0486f1741282
description: Sigma detection rule for an exploit attempt leveraging CVE-2023-23752
against 4.0.0 <= Joomla <= 4.2.7. This exploit is an information disclosure that
releases Mysql Credentials or the usernames and privileges of accounts active within
Joomla
status: experimental
date: 2023/04/04
modified: 2023/04/04
author: ZeroFox
tags:
  - attack.InitialAccess
  - mitre.T1190
references:
  -
https://developer.joomla.org/security-centre/894-20230201-core-improper-access-check-in-webservice-endpoints.html
logsource:
  product: linux
detection:
  logfile:
    - log.file.path: '*access*.log'
  mysql-cred-dump:
    event.original:
      - '*api/index.php/v1/config/application?public=true*' #matching on leaking
mysql password attempt
  useraccount-dump:
    event.original:
      - '*api/index.php/v1/users?public=true*' #matching on leaking user accounts
information
  condition: logfile and (mysql-cred-dump or useraccount-dump)
falsepositives:
  - Joomla instance version is not between 4.0.0 and 4.2.7
  - Other applications having the same endpoints
level: High
```

Figure 2. Sigma Rules to detect CVE-2023-23752

Source: ZeroFox Intelligence Collections



Appendix 2: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.