The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
04/26/2022

SUBJECT:
A Vulnerability in WSO2 Products Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in specific WSO2 products, which could allow for remote code execution. WSO2 is an open-source technology provider. It offers an enterprise platform for integrating application programming interfaces (API), applications, and web services locally and across the Internet. Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view; change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
A proof-of-concept exploit was posted to GitHub on April 20, 2022 and according to a Rapid7 report, cyber threat actors are using the proof-of-concept exploit to deploy web shells and coin miners. According to the same report, "The proof of concept uploads a malicious .jsp to /fileupload/toolsAny on the WSO2 product's webserver. The .jsp is a web shell, and due to a directory traversal issue affecting the upload files name, the attacker can write it to a location where they can then send it commands. The attack is not restricted to .jsp files."

The MS-ISAC is currently observing active exploitation of this vulnerability against U.S. higher education to deploy coin miners and potentially as an initial access vector in a ransomware attack. WSO2's website states that "Ethos Identity provides IAM capabilities for over 500 + universities globally. The underlying technology of Ellucian's Ethos Identity is WSO2 Identity Server making WSO2 IAM one of the most trusted IdPs/ IAM providers."

CISA recently included CVE-2022-29464 to their list of "Known Exploited Vulnerabilities Catalog" and is requiring federal agencies to apply associated patches and security updates by May, 16, 2022.

SYSTEMS AFFECTED:

- WSO2 API Manager 2.2.0 and above
- WSO2 Identity Server 5.2.0 and above
- WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, 5.6.0
- WSO2 Identity Server as Key Manager 5.3.0 and above
- WSO2 Enterprise Integrator 6.2.0 and above
- WSO2 Open Banking AM 1.4.0 and above
- WSO2 Open Banking KM 1.4.0 and above

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in certain WSO2 Platform products, which could allow for remote code execution. This vulnerability exists due to improper validation of user input, a malicious actor could upload an arbitrary file to a user controlled location of the server. By leveraging the vulnerability, a malicious actor may perform Remote Code Execution by uploading a specially crafted payload. The attacker must use a /fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a ../../../../repository/deployment/server/webapps directory. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Upgrade to the latest version of the product affected via the WSO2 Support Matrix.
- If remediation is not possible, remove installations from the public internet as soon as possible.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Verify no unauthorized system modifications have occurred on the system before applying the patch.

REFERENCES:

CVE:
https://www.cve.org/CVERecord?id=CVE-2022-29464

Rapid7:
https://www.rapid7.com/blog/post/2022/04/22/opportunistic-exploitation-of-wso2-cve-2022-29464/

WSO2:
https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738
https://wso2.com/updates/