

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

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

08/07/2020

SUBJECT:

Multiple Vulnerabilities in Apache Web Server Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apache web server, the most severe of which could allow for remote code execution. Apache web server is a piece of software developed by the Apache software foundation as a free open source tool used to host websites. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code in the context of the affected application. 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 these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Apache versions 2.4.43 and prior

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:

Multiple vulnerabilities have been discovered in Apache web server, the most severe of which could allow for remote code execution. These vulnerabilities can be triggered when specially crafted packets are submitted for processing to an affected web server. Details of the vulnerabilities are as follows:

- A possible remote code execution vulnerability due to a buffer overflow with the mod_uwsgi module. (CVE-2020-11984)
- A denial of service vulnerability triggered when trace/debugging is enabled. (CVE-2020-11993)
- A denial of service vulnerability triggered when a PUSH packet is sent using the 'Cache-Digest' header. (CVE-2020-9490)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute remote code in the context of the affected application. 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 these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply updates provided by Apache to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Configure the application as suggested by Apache to help mitigate the vulnerability.

REFERENCES:

Apache:

https://httpd.apache.org/security/vulnerabilities_24.html

CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11984>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11993>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9490>

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

<http://www.us-cert.gov/tlp/>