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:
03/22/2021

SUBJECT:
A Vulnerability in Adobe ColdFusion Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Adobe ColdFusion, which could allow for arbitrary code execution. Adobe ColdFusion is a web application development platform. Successful exploitation of this vulnerability could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- ColdFusion 2021 (Version 2021.0.0.323925)
- ColdFusion 2018 (Update 10 and earlier)
- ColdFusion 2016 (Update 16 and earlier)

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 Adobe ColdFusion, which could allow for arbitrary code execution. This vulnerability occurs due to improper input validation. Successful exploitation of this vulnerability could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user

rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Adobe:

https://helpx.adobe.com/security/products/coldfusion/apsb21-16.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21087