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:
06/11/2019

SUBJECT:
Multiple Vulnerabilities in Adobe ColdFusion Could Allow for Arbitrary Code Execution (APSB19-27)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe ColdFusion, the most severe of which could allow for arbitrary code execution. Adobe ColdFusion is a web application development platform. Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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 no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- ColdFusion 2018 for All versions prior to Update 3
- ColdFusion 2016 for All versions prior to Update 10
- ColdFusion 11 for All versions prior to Update 18

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 Adobe ColdFusion, the most severe of which could allow for arbitrary code execution. The details of these vulnerabilities are as follows:

- A File extension blacklist bypass vulnerability that could allow for Arbitrary code execution. (CVE-2019-7838)

- A Command Injection vulnerability that could allow for Arbitrary code execution. (CVE-2019-7839)
- A Deserialization of untrusted data vulnerability that could allow for Arbitrary code execution. (CVE-2019-7840)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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:

- 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 websites or follow links provided by unknown or untrusted 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/apsb19-27.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7838
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7839
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7840

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov