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:
07/11/2019

SUBJECT:
A Vulnerability in Jira Server Could Allow for Server-Side Template Injection

OVERVIEW:
A vulnerability has been discovered in JIRA Servers & Data Centers, which can allow for server template injection. JIRA is tool designed for bug tracking, tracking related issues and project management. Successful exploitation of this vulnerability will enable command injection to the vulnerable server. Depending on the privileges associated with the user running the Jira application service, 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 this vulnerability could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There is a publicly available exploit for this vulnerability.

SYSTEMS AFFECTED:

- JIRA Servers & Data Centers 7.x versions prior to 7.6.14 and 7.13.5
- JIRA Servers & Data Centers 8.0.x versions prior to 8.0.3
- JIRA Servers & Data Centers 8.1.x versions prior to 8.1.2
- JIRA Servers & Data Centers 8.2.x versions prior to 8.2.3

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 JIRA Servers & Data Centers, which can allow for server template injection. This vulnerability occurs when an SMTP server has been configured in Jira and a malicious user has access to either the “Contact Administrators Form” or has “JIRA Administrators” access. If an attacker has administrator access, they can exploit this vulnerability via Velocity Templates. This vulnerability exists due to improper input validation within the subject field. When an attacker sends a specially crafted payload to the subject field

within the “Contact Administrators Form” or the Velocity template, the desired command injected will be executed in the context of the server. Successful exploitation of this vulnerability will enable command injection to the vulnerable server.

Successful exploitation of this vulnerability will enable command injection to the vulnerable server. Depending on the privileges associated with the user running the Jira application service, 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 this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Jira 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.
- 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:

Atlassian:
https://confluence.atlassian.com/jira/jira-security-advisory-2019-07-10-973486595.html
https://jira.atlassian.com/browse/JRASERVER-69532?_ga=2.226002522.1185876089.1562812581-1154294990.1562812581

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11581

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/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

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

iTS Mississippi Department of
Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited