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:
05/28/2019

SUBJECT:
A Vulnerability in IBM WebSphere Application Server Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in IBM WebSphere Application Server that could allow for remote code execution. IBM WebSphere Application Server is a software framework and middleware that hosts Java-based web applications. Successful exploitation of this vulnerability 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 install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

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

SYSTEMS AFFECTED:

- WebSphere Application Server ND (Traditional and Hypervisor) version 9.0 through 9.0.0.11
- WebSphere Application Server ND (Traditional and Hypervisor) version 8.5.0.0 through 8.5.5.15
- WebSphere Virtual Enterprise version 7.0

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 IBM WebSphere Application Server that could allow for remote code execution. This issue occurs when serializing an object from an untrusted source. This could allow for a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects.

Successful exploitation of this vulnerability 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 install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to the latest version of IBM WebSphere Application Server immediately, after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.

REFERENCES:

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-4279

IBM:

https://www-01.ibm.com/support/docview.wss?uid=ibm10883628

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/

Greg Nohra
Enterprise Security Architect
MS Department of Information Technology Services
601-432-8009 | 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