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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
12/10/2021
12/13/2021 - UPDATED
12/14/2021 - UPDATED

SUBJECT:
A Vulnerability in Apache Log4j Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Apache Log4j, a very ubiquitous logging package for Java. Successful exploitation of this vulnerability could allow for arbitrary code execution within the context of the systems and services that use the Java logging library, including many services and applications written in Java. Depending on the privileges associated with these systems and services, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If these systems and services have been configured to have fewer user rights, exploitation of this vulnerability could have less impact than if they were configured with administrative rights.

THREAT INTELLIGENCE:
According to numerous open source reports, Log4j is used with Apache software like Apache Struts, Solr, Druid, along with other technologies. Many websites of manufacturers and providers have been found to be affected including Apple, Twitter, Steam, Tesla and more. Threat actors will likely include payloads in simple HTTP connections, either in a User-Agent header or trivial POST form data. In addition, it has been reported that organizations are already seeing signs of exploitation in the wild with further attempts on other websites likely.

SYSTEMS AFFECTED:
- Apache Log4j between versions 2.0 and 2.14.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability has been discovered in Apache Log4j, a very ubiquitous logging package for Java. This vulnerability resides in the JNDI lookup feature of the log4j library. The JNDI lookup feature of log4j allows variables to be retrieved via JNDI - Java Naming and Directory Interface. This is an API that provides naming and directory functionality to Java applications. While there are many possibilities, the log4j API supports LDAP and RMI (Remote Method Invocation). An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Successful exploitation of this vulnerability could allow for arbitrary code execution within the context of the systems and services that use the Java logging library, including many services and applications written in Java. Depending on the privileges associated with these systems and services, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If these systems and services have been configured to have fewer user rights, exploitation of this vulnerability could have less impact than if they were configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the latest patches (version 2.15.0) provided by Apache after appropriate testing.
- Run all systems and services as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

December 13 - UPDATED RECOMMENDATIONS:

- Run the “Log4Shell” Vulnerability Tester provided by Huntress to test whether your applications are vulnerable to CVE-2021-44228 (please see references for the Huntress link).
- Check the GitHub repository listed in the reference section to see all the Security Advisories & Bulletins related to CVE-2021-44228, which include applications affected, version numbers, and the associated patches that should be implemented if you have the affected version in your environment.

December 14 - UPDATED RECOMMENDATIONS:

- ***The previous patch iteration 2.15.0 does not fully remediate the vulnerability, and thus it is recommended to apply the latest patch (version 2.16.0)***

REFERENCES:

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

SANS Technology Institute:
https://isc.sans.edu/diary/28120

ZDNet:
https://www.zdnet.com/article/security-warning-new-zero-day-in-the-log4j-java-library-is-already-being-exploited/

Ars Technica:

https://arstechnica.com/information-technology/2021/12/minecraft-and-other-apps-face-serious-threat-from-new-code-execution-bug/

December 13 - UPDATED REFERECENCES:

GitHub:
https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

Huntress Log4Shell Tool:
https://log4shell.huntress.com/

December 14 - UPDATED REFERECENCES:
Apache:
https://logging.apache.org/log4j/2.x/

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.