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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
07/29/2022

SUBJECT:
A Vulnerability in the Grails Framework Could Allow for Remote Code Execution (CVE-2022-35912)

OVERVIEW:
A vulnerability have been discovered in the Grails Framework which could allow for remote code execution. Grails is backend Apache Groovy framework. Successful exploitation of this vulnerability, could allow a user to execute code in the context of the Grails application.

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

SYSTEMS AFFECTED:

- Grails framework versions
  - >= 3.3.10 & < 3.3.15
  - >= 4.0.0 & < 4.1.1
  - >= 5.0.0 & < 5.1.9
  - 5.2.0

- Running on Java 8

- Using embedded Tomcat runtime, as well as those deployed to a Servlet Container

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: Low

TECHNICAL SUMMARY:
A vulnerability have been discovered in the Grails Framework (CVE-2022-35912) which could allow for remote code execution. Details of this vulnerability are as follows:

Tactic: *Execution* (TA00041):

Technique: *Native Code* (T1575):

- CVE-2022-35912 – A vulnerability in a section of the Grails data-binding logic which enables an attack to issue a specially crafted web request to execute code of their own choosing.

Successful exploitation of this vulnerability, could allow a user to execute code in the context of the Grails application.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by the Grails team to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
  - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources. (**M1017: User Training**)
  - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise’s workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

  - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection)**

Safeguard 10.5: Enable anti-exploitation features on enterprise assets and software, where possible, such as Apple® System Integrity Protection (SIP) and Gatekeeper™.

REFERENCES:

Grails:https://grails.org/blog/2022-07-18-rce-vulnerability.html

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35912