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:
06/10/2022

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the logged-on user. Depending on the privileges associated with the logged-on user, an attacker could view, change, or delete data. If the logged-on user has been configured to have fewer rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if they were configured with administrative rights.

THREAT INTELLIGENCE:
There are no reports that these vulnerabilities are being exploited in the wild.

SYSTEMS AFFECTED:

- Google Chrome for Windows, Mac and Linux versions prior to 102.0.5005.115

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:
Multiple vulnerabilities have been discovered in Chrome, the most severe of which could allow for arbitrary code execution. Following the MITRE ATT&CK framework, exploitation of these vulnerabilities can be classified as follows :

Tactic: *Initial Access* **(**TA0001**)**:

Technique: *Drive-by Compromise* **(**T1189**)**:

- Use after free in WebGPU. (CVE-2022-2007)
- Use after free in ANGLE. (CVE-2022-2011)
- Out of bounds memory access in WebGL. (CVE-2022-2008)
- Out of bounds read in Compositing. (CVE-2022-2010)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the logged-on user. Depending on the privileges associated with the logged-on user, an attacker could view, change, or delete data. If the logged-on user 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 they were configured with administrative rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply the stable channel update provided by Google 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 the 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.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Google:
https://chromereleases.googleblog.com/2022/06/stable-channel-update-for-desktop.html

US-CERT:
https://www.cisa.gov/uscert/ncas/current-activity/2022/06/10/google-releases-security-updates-chrome

CISA:
https://us-cert.cisa.gov/ncas/current-activity/2022/06/10/google-releases-security-updates-chrome

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2011