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:
08/16/2022

SUB6JECT:
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 for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights

THREAT INTELLIGENCE:
Google is aware that an exploit for CVE-2022-2856 exists in the wild.

SYSTEMS AFFECTED:

- Chrome for Windows versions prior to 104.0.5112.102/101
- Chrome for Mac and Linux versions prior to 104.0.5112.101

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:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

Tactic: *Initial Access* **(**TA0002**):**

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

- Use after free in FedCM. (CVE-2022-2852)
- Use after free in SwiftShader. (CVE-2022-2854)
- Use after free in ANGLE. (CVE-2022-2855)
- Use after free in Blink. (CVE-2022-2857)
- Use after free in Sign-In Flow. (CVE-2022-2858)
- Heap buffer overflow in Downloads. (CVE-2022-2853)
- Insufficient validation of untrusted input in Intents. (CVE-2022-2856)

Details of lower-severity vulnerabilities are as follows:

- Use after free in Chrome OS Shell. (CVE-2022-2859)
- Insufficient policy enforcement in Cookies. (CVE-2022-2860)
- Inappropriate implementation in Extensions API. (CVE-2022-2861)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user 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.

- 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.
- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)
    - **Safeguard 9.2: Use DNS Filtering Services:** Use DNS filtering services on all enterprise assets to block access to known malicious domains.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
- Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction. **(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 14.6:** Train Workforce Members on Recognizing and Reporting Security Incidents: Train workforce members to be able to recognize a potential incident and be able to report such an incident.

REFERENCES:

Google:
https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2852

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2853
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2854

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2855 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2856

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2857

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2859

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2860

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2861