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:
03/02/2022

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 browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application 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 it was configured with administrative rights.

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

SYSTEMS AFFECTED:
- Google Chrome versions prior to 99.0.4844.51

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:

- CVE-2022-0789: Heap buffer overflow in ANGLE
- CVE-2022-0790: Use after free in Cast UI
- CVE-2022-0791: Use after free in Omnibox
- CVE-2022-0792: Out of bounds read in ANGLE
- CVE-2022-0793: Use after free in Views
- CVE-2022-0794: Use after free in WebShare
- CVE-2022-0795: Type Confusion in Blink Layout
- CVE-2022-0796: Use after free in Media. Reported by Cassidy Kim of Amber Security Lab
- CVE-2022-0797: Out of bounds memory access in Mojo
- CVE-2022-0798: Use after free in MediaStream
- CVE-2022-0799: Insufficient policy enforcement in Installer
- CVE-2022-0800: Heap buffer overflow in Cast UI
- CVE-2022-0801: Inappropriate implementation in HTML parser
- CVE-2022-0802: Inappropriate implementation in Full screen mode
- CVE-2022-0803: Inappropriate implementation in Permissions
- CVE-2022-0804: Inappropriate implementation in Full screen mode
- CVE-2022-0805: Use after free in Browser Switcher
- CVE-2022-0806: Data leak in Canvas
- CVE-2022-0807: Inappropriate implementation in Autofill
- CVE-2022-0808: Use after free in Chrome OS Shell
- CVE-2022-0809: Out of bounds memory access in WebXR

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application 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 it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the stable channel update provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- 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.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Google:

https://learn.cisecurity.org/e/799323/hannel-update-for-desktop-html/qvh4y/267149770?h=KK0dtLxbrV6vR6gpIWDCZgdWzVVIaePsWN1NHgOzIvQ

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0789
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0790
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0791
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0792
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0793
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0794
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0795
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0796
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0798
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0800
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0801
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0802
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0803
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0804
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0807
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0808
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0809