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:
05/10/2022
05/11/2022 - UPDATED

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

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome and ChromeOS, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Chrome OS is a proprietary Linux-based operating system designed by Google. It is derived from the open-source Chromium OS and uses the Google Chrome web browser as its principal user interface. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the applications. Depending on the privileges associated with the applications, an attacker could view, change, or delete data. If these applications have 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.

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

SYSTEMS AFFECTED:

- Google Chrome for Android versions prior to 101.0.4951.61
- ChromeOS versions prior to 101.0.4951.59

May 11th - UPDATED SYSTEMS AFFECTED:

- Google Chrome for Desktop versions prior to 101.0.4951.64

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 and ChromeOS, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- Chrome for Android
  - Use after free in Sharesheet. (CVE-2022-1633)
  - Use after free in Browser UI. (CVE-2022-1634)
  - Use after free in Permission Prompts. (CVE-2022-1635)
  - Use after free in Performance APIs. (CVE-2022-1636)
  - Inappropriate implementation in Web Contents. (CVE-2022-1637)
  - Heap buffer overflow in V8 Internationalization. (CVE-2022-1638)
  - Use after free in ANGLE. (CVE-2022-1639)
  - Use after free in Sharing.(CVE-2022-1640)
  - Use after free in Web UI Diagnostics. (CVE-2022-1641)
- ChromeOS
  - Heap Use-after-free in Window Manager
  - Use after free in Chrome OS shell.
  - Heap buffer overflow in Window Manager.
  - Use-after-free in file selection dialog
  - Use-after-free in PPD file selection dialog
  - Use-after-free in file selection dialog
  - Buffer overflow in Shelf

May 11h – UPDATED TECHNCAL SUMMARY:

- Chrome for Desktop
  - Use after free in Sharesheet. (CVE-2022-1633)
  - Use after free in Browser UI. (CVE-2022-1634)
  - Use after free in Permission Prompts. (CVE-2022-1635)

- Use after free in Performance APIs. (CVE-2022-1636)
- Inappropriate implementation in Web Contents. (CVE-2022-1637)
- Heap buffer overflow in V8 Internationalization. (CVE-2022-1638)
- Use after free in ANGLE. (CVE-2022-1639)
- Use after free in Sharing.(CVE-2022-1640)
- Use after free in Web UI Diagnostics. (CVE-2022-1641)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the applications. Depending on the privileges associated with the applications, an attacker could view, change, or delete data. If these applications have 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.
- 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://chromereleases.googleblog.com/

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1633

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1634

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1635

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1636

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1637

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1638

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1639

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1640

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1641

May 11th – UPDATED REFERANCES:

Google:https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html