

*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](http://www.cisa.gov/tlp)

**Information may be distributed without restriction, subject to standard copyright rules.**

**DATE(S) ISSUED:**

03/30/2022

**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 100.0.4896.60

**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 Google Chrome, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- CVE-2022-1125: Use after free in Portals
- CVE-2022-1127: Use after free in QR Code Generator
- CVE-2022-1128: Inappropriate implementation in Web Share API
- CVE-2022-1129: Inappropriate implementation in Full Screen Mode
- CVE-2022-1130: Insufficient validation of untrusted input in WebOTP
- CVE-2022-1131: Use after free in Cast UI
- CVE-2022-1132: Inappropriate implementation in Virtual Keyboard
- CVE-2022-1133: Use after free in WebRTC
- CVE-2022-1134: Type Confusion in V8
- CVE-2022-1135: Use after free in Shopping Cart
- CVE-2022-1136: Use after free in Tab Strip
- CVE-2022-1137: Inappropriate implementation in Extensions
- CVE-2022-1138: Inappropriate implementation in Web Cursor
- CVE-2022-1139: Inappropriate implementation in Background Fetch API
- CVE-2022-1141: Use after free in File Manager
- CVE-2022-1142: Heap buffer overflow in WebUI
- CVE-2022-1143: Heap buffer overflow in WebUI
- CVE-2022-1144: Use after free in WebUI
- CVE-2022-1145: Use after free in Extensions
- CVE-2022-1146: Inappropriate implementation in Resource Timing

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:

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/2022/03/stable-channel-update-for-desktop\\_29.html](https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_29.html)

##### CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1125>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1127>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1128>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1129>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1130>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1131>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1132>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1133>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1134>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1135>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1136>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1137>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1138>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1139>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1141>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1142>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1143>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1144>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1145>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1146>