TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
05/11/2021

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 currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome versions prior to 90.0.4430.212

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. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- An incorrect security UI vulnerability exists in the 'Webb App Installs' component. (CVE-2021-30506)

- An inappropriate implementation vulnerability exists in the 'Offline' component. (CVE-2021-30507)
- A heap buffer overflow vulnerability exists in the 'Media Feeds' component. (CVE-2021-30508)
- An out of bounds write vulnerability exists in the 'Tab Strip' component. (CVE-2021-30509)
- A race vulnerability exists in the 'Aura' component. (CVE-2021-30510)
- An out of bounds read vulnerability exists in the 'Tab Groups' component. (CVE-2021-30511)
- A use-after-free vulnerability exists in the 'Notifications' component. (CVE-2021-30512)
- A type confusion vulnerability exists in the 'V8' component. (CVE-2021-30513)
- A use-after-free vulnerability exists in the 'Autofill' component. (CVE-2021-30514)
- A use-after-free vulnerability exists in the 'File API component'. (CVE-2021-30515)
- A heap buffer overflow vulnerability exists in the 'History' component. (CVE-2021-30516)
- A type confusion vulnerability exists in the 'V8' component. (CVE-2021-30517)
- A heap buffer overflow vulnerability exists in the 'Reader Mode' component. (CVE-2021-30518)
- A use-after-free vulnerability exists in the 'Payments' component. (CVE-2021-30519)
- A use-after-free vulnerability exists in the 'Tab Strip' component. (CVE-2021-30520)

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 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/2021/05/stable-channel-update-for-desktop.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30506
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30507
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30508
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30509
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30510
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30511

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30512
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30515
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30517
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30519
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30520