Hive Pro

THREAT ADVISORY

Google Chrome affected by high severity vulnerabilities	TA2022026
Threat Level GREEN	**Publish Date –** Feb 10, 2022

Google has released Chrome 98 as a stable channel for Windows, Mac, and Linux. This update addresses 19 security vulnerabilities. Eight of them are rated severity high, ten of them are medium and one of them is of severity low. This advisory highlights the high impact vulnerabilities.

Five of the eight high-rated Chrome vulnerabilities are impacted by Use-After-Free (UAF) flaw. This is a vulnerability related to incorrect use of dynamic memory during program operation. Successful exploitation of this issue may lead to data corruption, program crash or arbitrary code execution. In recent browser versions a number of controls have been introduced that make exploitation of these use after free vulnerabilities much harder but despite this, they still seem to persist.

Other prominent attacks in this release are heap buffer overflow that affects the Chrome V8 engine. V8 is an open-source JavaScript engine which is used by Google Chrome and Chromium-based web browsers like Microsoft Edge, Opera, Amazon Silk, Brave, Yandex and Vivaldi. Attackers may carry out this attack to gain access to information that is otherwise off limits to them, or to execute arbitrary code on the device.

Organizations should update to Chrome 98.0.4758.80/81/82 for Windows and 98.0.4758.80 for Mac and Linux to avoid exploitation.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0452	Google Chrome prior to Chrome 98.0.4758.80	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in Safe Browsing.	CWE-416
CVE-2022-0453			Use after free in Reader Mode.	CWE-416
CVE-2022-0454			Heap buffer overflow in ANGLE.	CWE-122
CVE-2022-0455			Inappropriate implementation in Full Screen Mode.	CWE-358
CVE-2022-0456			Use after free in Web Search.	CWE-416
CVE-2022-0457			Type Confusion in V8.	CWE-843
CVE-2022-0458			Use after free in Thumbnail Tab Strip.	CWE-416
CVE-2022-0459			Use after free in Screen Capture.	CWE-416

Patch Link

https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html?m=1

References

https://www.forbes.com/sites/gordonkelly/2022/02/02/google-chrome-hack-vulnerability-attack-free-chrome-98-upgrade/?sh=6563b9d74225