Hive Pro

THREAT ADVISORY

First zero-day vulnerability of Google Chrome this year actively exploited in wild

TA2022033

Threat Level RED

Publish Date – Feb 15, 2022

Google released a stable channel update for their Chrome browser that contains a zero-day vulnerability and is actively being exploited-in-wild. This is the first zero-day bug reported in Chrome browser this year.

A Use-After-Free (UAF) vulnerability which has been assigned CVE-2022-0609 affects the Animation component that may allow attackers to corrupt data, crash program or execute arbitrary code on computers running unpatched Chrome versions or escape the browser's security sandbox. 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.

In addition to the zero-day bug, this update fixed seven other security vulnerabilities as mentioned in the table below. We recommend organizations to update to Chrome 98.0.4758.102 for Windows, Mac and Linux to avoid exploitation and mitigate any potential threats.

Potential MITRE ATT&CK TTPs are:
TA0040 - Impact
TA0001 - Initial Access
TA0002 - Execution
T1499- Endpoint Denial of Service
T1189- Drive-by Compromise
T1190- Exploit-public facing application
T1203- Exploitation for Client Execution
T1499.004- Endpoint Denial of Service: Application or System Exploitation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0603	Google Chrome prior to Chrome 98.0.4758.80	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	Use after free in File Manager	CWE-416
CVE-2022-0604			Heap buffer overflow in Tab Groups	CWE-122
CVE-2022-0605			Use after free in Webstore API	CWE-416
CVE-2022-0606			Use after free in ANGLE	CWE-416
CVE-2022-0607			Use after free in GPU	CWE-416
CVE-2022-0608			Integer overflow in Mojo	CWE-190
CVE-2022-0609			Use after free in Animation	CWE-416
CVE-2022-0610			Inappropriate implementation in Gamepad API	CWE-358

Patch Link

https://www.google.com/intl/en/chrome/?standalone=1

References

https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html