Hive Pro

THREAT ADVISORY

Google Chrome issues an emergency update to address the third zero-day of year 2022

TA2022092

Threat Level RED

Publish Date – April 15, 2022

A zero-day vulnerability has been discovered in Google Chrome versions prior to 100.0.4896.127. A type of confusion vulnerability tracked as CVE-2022-1364, is said to be exploited in the wild.

This vulnerability affects the V8 component, which is used to parse JavaScript code in Google Chrome. A type of confusion refers to code errors in which an app begins data execution processes with a given "type" of input but is deceived into considering the input as a different "type". The "type confusion" causes logical mistakes in the memory of the software. Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code in the context of the browser.

We recommend organizations update to Chrome 100.0.4896.127 for Windows, Mac and Linux to avoid exploitation and mitigate any potential threats.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
TA0001: Initial Access
T1190: Exploit Public-Facing Application

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-1364	Google Chrome: 70.0.3538.67 - 100.0.4896.127	cpe:2.3:a:google:google_chrome:*:*:*:*:*:*:*:*	Type Confusion in V8	CWE-843

Patch Links

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

References

https://chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop_14.html