Multiple Vulnerabilities in Google Chrome

Severity Level: High

Components Affected

- Google Chrome prior to 120.0.6099.224 (Linux)
- Google Chrome prior to 120.0.6099.234 (Mac)
- Google Chrome prior to 120.0.6099.224/225 (Windows)

Overview

Multiple vulnerabilities were identified in Google Chrome. Where a remote attacker could exploit some of these vulnerabilities to trigger denial of service condition, remote code execution and sensitive information disclosure on the targeted system.

Description

Multiple vulnerabilities have been discovered in Google Chrome and an actively exploited zero-day vulnerability tracked by CVE-2024-0519. Details of these severe vulnerabilities are as follows:

- CVE-2024-0517: Out of bounds write in V8.
- CVE-2024-0518: Type Confusion in V8.
- CVE-2024-0519: Out-of-bounds memory access in the V8 JavaScript and WebAssembly engine, which can be weaponized by threat actors to trigger a crash.

Impact

- Remote Code Execution
- Denial of Service
- Information Disclosure

Solution/ Workarounds

Before installation of the software, please visit the software vendor web-site for more details.

Apply fixes issued by the vendor:

- Update to version 120.0.6099.224 (Linux) or later
- Update to version 120.0.6099.234 (Mac) or later
- Update to version 120.0.6099.224/225 (Windows) or later

Reference

- https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html
- https://thehackernews.com/2024/01/zero-day-alert-update-chrome-now-to-fix.html

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.