Multiple Vulnerabilities in Google Chrome

Severity Level: High

Components Affected

- Google Chrome prior to 119.0.6045.199 (Linux)
- Google Chrome prior to 119.0.6045.199 (Mac)
- Google Chrome prior to 119.0.6045.199/.200 (Windows)

Overview

Multiple vulnerabilities were identified in Google Chrome, where a remote attacker could exploit some of these vulnerabilities to trigger security restriction bypass, data manipulation, remote code execution and denial of service condition on the targeted system.

Description

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for remote code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Details of these severe vulnerabilities are as follows:

- Heap buffer overflow in vp8 encoding in libvpx. (CVE-2023-5217)
- Use after free in Extensions. (CVE-2023-51872)
- Use after free Passwords. (CVE-2023-5186)

Impact

- Remote Code Execution
- Denial of Service
- Security Restriction Bypass
- Data Manipulation

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 119.0.6045.199 (Linux) or later
- Update to version 119.0.6045.199 (Mac) or later
- Update to version 119.0.6045.199/.200 (Windows) or later

Reference

- https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Disclaimer

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