Multiple Vulnerabilities in Google Chrome

Severity Level: High

Components Affected

- Google Chrome prior to 118.0.5993.70 (Linux)
- Google Chrome prior to 118.0.5993.70 (Mac)
- Google Chrome prior to 118.0.5993.70/.71 (Windows)

Overview

Multiple vulnerabilities were identified in Google Chrome. A remote attacker could exploit some of these vulnerabilities to trigger information disclosure, remote code execution and privilege escalation on the targeted system.

Description

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary 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.

Impact

- Remote Code Execution
- Information Disclosure
- Privilege Escalation

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 118.0.5993.70 (Linux) or later
- Update to version 118.0.5993.70 (Mac) or later
- Update to version 118.0.5993.70/.71 (Windows) or later

Reference

- https://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop_10.html
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-121

Disclaimer

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