Multiple Vulnerabilities in Google Chrome

Severity Level: High

Components Affected

- Google Chrome prior to 117.0.5938.62 (Linux)
- Google Chrome prior to 117.0.5938.62 (Mac)
- Google Chrome prior to 117.0.5938.62/.63 (Windows)
- Google Chrome prior to 117.0.5938.60 (Android)

Overview

Multiple vulnerabilities have been identified in Google Chrome, whereby a remote attacker could potentially exploit these vulnerabilities to trigger a denial-of-service condition, elevate privileges, execute remote code, and bypass security restrictions on the targeted system.

Description

The primary vulnerability is the remote code execution vulnerability, which has been identified and tracked under CVE-2023-4863. This vulnerability could be exploited through a heap buffer overflow in WebP, potentially leading to arbitrary code execution and enabling attackers to perform denial-of-service attacks.

Impact

- Remote Code Execution
- Denial of Service
- Elevation of Privilege
- Security Restriction Bypass

Solution/ Workarounds

Apply fixes issued by the vendor by updating to the latest versions mentioned below:

- Update to version 117.0.5938.62 (Linux) or later
- Update to version 117.0.5938.62 (Mac) or later
- Update to version 117.0.5938.62/.63 (Windows) or later
- Update to version 117.0.5938.60 (Android) or later

Reference

- https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerability_20230912

Disclaimer

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