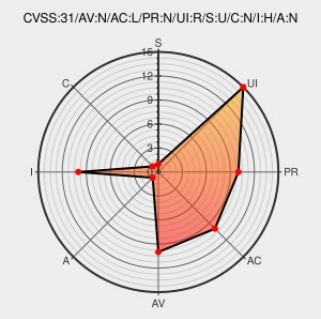
CVE-2020-6506

Published on: 07/22/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-6506

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Android from Google contain the following vulnerability:

Insufficient policy enforcement in WebView in Google Chrome on Android prior to 83.0.4103.106 allowed a remote attacker to bypass site isolation via a crafted HTML page.

CVE-2020-6506 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 83.0.4103.106**

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Pony Mail!	Mailing List Third Party Advisory	MLIST [cordova-issues] 20200929 [GitHub] [cordova-docs] purplecabbage merged pull request #1123: Added Security

	lists.apache.org text/html	purplecabbage merged pull request #1123: Added Security Advisory CVE-2020-6506
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202007-08) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-202007-08
Pony Mail!	Mailing List Third Party Advisory lists.apache.org text/html	MLIST [cordova-issues] 20200929 [GitHub] [cordova-docs] purplecabbage opened a new pull request #1123: Added Security Advisory CVE-2020-6506
Pony Mail!	Mailing List Third Party Advisory lists.apache.org text/html	MLIST [cordova-issues] 20201001 [GitHub] [cordova-docs] dpogue commented on issue #1022: Document warnings on using remote source for
1083819 - chromium - An open-source project to help move the web forward. - Monorail	Issue Tracking Permissions Required Third Party Advisory crbug.com text/html	MISC crbug.com/1083819
Pony Mail!	Mailing List Third Party Advisory lists.apache.org text/html	MLIST [cordova-issues] 20201007 [GitHub] [cordova-plugin-inappbrowser] carlpoole opened a new pull request #792: fix(android): Add mitigation strategy for CVE-2020-6506
Pony Mail!	Mailing List Patch Third Party Advisory lists.apache.org text/html	MLIST [cordova-commits] 20201117 [cordova-plugin-inappbrowser] branch master updated: fix(android): Add mitigation strategy for CVE-2020-6506 (#792)
Qt WebEngine: Multiple vulnerabilities (GLSA 202101-30) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-202101-30
Chrome Releases: Stable Channel Update for Desktop	Vendor Advisory chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_15.html
Pony Mail!	Mailing List Third Party Advisory lists.apache.org text/html	MLIST [cordova-issues] 20201117 [GitHub] [cordova-plugin-inappbrowser] NiklasMerz merged pull request #792: fix(android): Add mitigation strategy for CVE-2020-6506
Pony Mail!	Mailing List Third Party Advisory lists.apache.org text/html	MLIST [cordova-issues] 20201116 [GitHub] [cordova-plugin-inappbrowser] NiklasMerz commented on pull request #792: fix(android): Add mitigation strategy for CVE-2020-6506

Related QID Numbers

500849 Alpine Linux Security Update for chromium

980507 Nodejs (npm) Security Update for react-native-webview (GHSA-36j3-xxf7-4pqg)

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@AlesandroOrtizR	Why are all CVE pages returning 404s after a delay? e.g. Everythi… twitter.com/i/web/status/1…	2021-05-14 02:05:16
@OPOSEC	Universal XSS in Android WebView (CVE-2020-6506). alesandroortiz.com/articles/uxss-… More: hackerone.com/reports/906433 #Security #347 (2020)	2022-05-31 07:00:02
@AlesandroOrtizR	This was initially found by @__Sam0_0 using my PoC for CVE-2020-6506. Really appreciate their work here!	2022-07-29 02:40:33
@AlesandroOrtizR	@joaxcar It's a great area to research. CVE-2020-6506 also involved unexpected interactions between iframes and to… twitter.com/i/web/status/1…	2022-07-29 22:30:23

← Previous ID

Next ID→