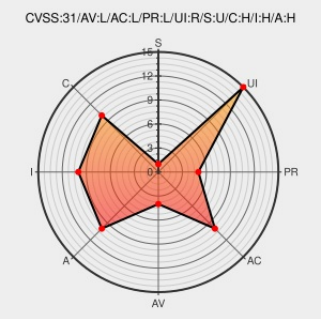
CVE-2023-0460

Published on: Not Yet Published

Last Modified on: 03/09/2023 12:56:00 AM UTC

CVE-2023-0460

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



Certain versions of Youtube Android Player Api from Google contain the following vulnerability:

The YouTube Embedded 1.2 SDK binds to a service within the YouTube Main App. After binding, a remote context is created with the flags Context.CONTEXT_INCLUDE_CODE | Context.CONTEXT_IGNORE_SECURITY. This allows the client app to remotely load code from YouTube Main App by retrieving the Main App's ClassLoader. A potential vulnerability in the binding logic used by the client SDK where the SDK ends up calling bindService() on a malicious app rather than YT Main App. This creates a vulnerability where the SDK can load the malicious app's ClassLoader instead, allowing the malicious app to load arbitrary code into the calling app whenever the embedded SDK is invoked. In order to trigger this vulnerability, an attacker must masquerade the Youtube app and install it on a device, have a second app that uses the Embedded player and typically distribute both to the victim outside of the Play Store.

CVE-2023-0460 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google** - **YouTube Android Player API SDK** version **<= 1.2.2**

CVSS3 Score: 7.3 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
YouTube Android Player API - Download | Google Developers	developers.google.com text/html	MISC developers.google.com/youtube/android/player/downloads

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Youtube Android Player Api	All	All	All	All

cpe:2.3:a:google:youtube_android_player_api:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-0460 : The YouTube Embedded 1.2 SDK binds to a service within the YouTube Main App. After binding, a remot… twitter.com/i/web/status/1…	2023-03-01 17:05:36

← Previous ID

Next ID→