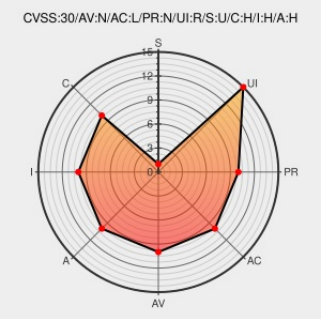
CVE-2019-2107

Published on: 07/08/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:04 PM UTC

CVE-2019-2107

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



Certain versions of Android from Google contain the following vulnerability:

In ihevcd_parse_pps of ihevcd_parse_headers.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130024844.

CVE-2019-2107 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Android Security Bulletin—July 2019 | Android Open Source Project	Vendor Advisory source.android.com	CONFIRM source.android.com/security/bulletin/2019-07-01

	text/html	
Android VideoPlayer ihevcd_parse_pps Out-Of-Bounds Write ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/153628/Android-VideoPlayer-ihevcd_parse_pps-Out-Of-Bounds-Write.html
Full Disclosure: CVE-2019-2107 a.k.a "Hevcfright" Proof of Concept exploit (Denial of Service PoC)	seclists.org text/html	FULLDISC 20190716 CVE-2019-2107 a.k.a "Hevcfright" Proof of Concept exploit (Denial of Service PoC)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All
Operating System	Google	Android	8.0	All	All	All
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All
Operating System	Google	Android	8.0	All	All	All
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All

cpe:2.3:o:google:android:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→