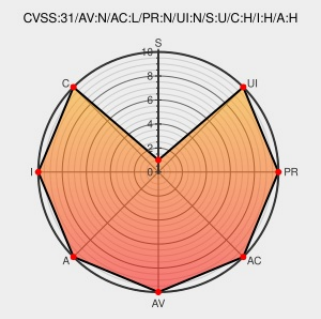
CVE-2020-12753

Published on: 05/11/2020 12:00:00 AM UTC

Last Modified on: 04/26/2022 07:54:00 PM UTC

CVE-2020-12753

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



Certain versions of Android from Google contain the following vulnerability:

An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. Arbitrary code execution can occur via the bootloader because of an EL1/EL3 coldboot vulnerability involving raw_resources. The LG ID is LVE-SMP-200006 (May 2020).

CVE-2020-12753 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
LG Product Security	Vendor Advisory, lgsecurity.lge.com, text/html	CONFIRM lgsecurity.lge.com/
[Segmentation Fault]	douevenknow.us	MISC douevenknow.us/post/619763074822520832/an-

	text/html	el1el3-coldboot-vulnerability
New cold boot attack affects seven years of LG Android smartphones | ZDNet	www.zdnet.com text/html	MISC www.zdnet.com/article/new-cold-boot-attack-affects-seven-years-of-lg-android-smartphones/

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

Exploit/POC from Github

A proof-of-concept for CVE-2020-12753

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	10.0	All	All	All
Operating System	Google	Android	7.2	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	10.0	All	All	All
Operating System	Google	Android	7.2	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:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.2:*:*:*:*:*:*:*:

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:10.0:*:*:*:*:*:*:*

cpe:2.3:o:google:android:7.2:*:*:*:*:*:*:*

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

Social Mentions

Source	Title	Posted (UTC)
@Hs0ci3ty	@jonathandata1 @Zerodium @LGUS Aight well I wish it is either CVE-2020-12753 or qmi.	2021-10-09 15:17:32
@RemotelyAlerts	Severity: ??? | An issue was discovered on LG mobile dev... | CVE-2020-12753 | Link for more: alerts.remotelyrmm.com/CVE-2020-12753	2022-04-26 21:33:33

← Previous ID

Next ID→