

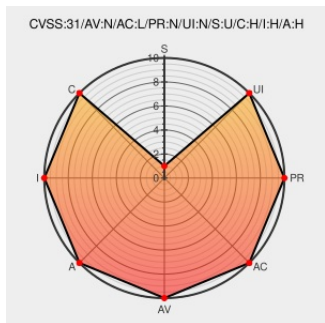


CVE-2020-8899

Published on: 05/06/2020 12:00:00 AM UTC

Last Modified on: 10/07/2022 12:21:00 AM UTC

CVE-2020-8899

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

There is a buffer overwrite vulnerability in the Quram qmg library of Samsung's Android OS versions O(8.x), P(9.0) and Q(10.0). An unauthenticated, unauthorized attacker sending a specially crafted MMS to a vulnerable phone can trigger a heap-based buffer overflow in the Quram image codec leading to an arbitrary remote code execution (RCE) without any user interaction. The Samsung ID is SVE-2020-16747.

CVE-2020-8899 has been assigned by [Google](#) security@google.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Samsung](#) - **Android OS** version **>= 8.x**

Affected Vendor/Software: [Samsung](#) - **Android OS** version **= 9.0**

Affected Vendor/Software: [Samsung](#) - **Android OS** version **= 10.0**

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: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
2002 - project-zero - Project Zero - Monorail	Exploit Third Party Advisory bugs.chromium.org text/html	 CONFIRM bugs.chromium.org/p/project-zero/issues/detail?id=2002
VU#366027 - Samsung Qmage codec for Android Skia library does not properly validate image files	www.kb.cert.org text/html	 CERT-VN VU#366027
Samsung Android Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/157620/Samsung-Android-Remote-Code-Execution.html
Samsung Mobile Security	Vendor Advisory security.samsungmobile.com text/html	 CONFIRM security.samsungmobile.com/securityUpdate.smsb

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
Operating System	Google	Android	10.0	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	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:8.0:*****:.*						
cpe:2.3:o:google:android:8.1:*****:.*						
cpe:2.3:o:google:android:9.0:*****:.*						

cpe:2.3:o:google:android:8.0:*:*:*:*:*:
cpe:2.3:o:google:android:10.0:*:*:*:*:*:
cpe:2.3:o:google:android:8.0:*:*:*:*:*:
cpe:2.3:o:google:android:8.1:*:*:*:*:*:
cpe:2.3:o:google:android:9.0:*:*:*:*:*:

Discovery Credit

Mateusz Jurczyk of Google Project Zero

Social Mentions		
Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ??? There is a buffer overwrite vulnerabilit... CVE-2020-8899 Link for more: alerts.remotelyrmm.com/CVE-2020-8899	2022-10-07 01:32:15
← Previous ID		Next ID →