

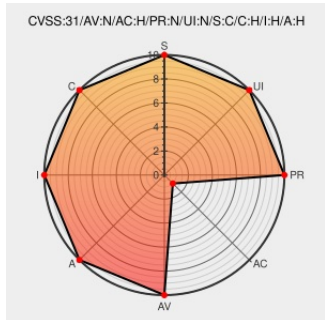


CVE-2021-25385

Published on: 06/11/2021 12:00:00 AM UTC

Last Modified on: 09/23/2022 07:12:00 PM UTC

CVE-2021-25385

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

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

An improper input validation vulnerability in `sdfffd_parse_chunk_PROP()` in `libsdfextractor` library prior to SMR MAY-2021 Release 1 allows attackers to execute arbitrary code on `mediaextractor` process.

CVE-2021-25385 has been assigned by [S](#) `mobile.security@samsung.com` to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [S](#) **Samsung Mobile - Samsung Mobile Devices** version < **SMR MAY-2021 Release 1**

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
Samsung Mobile Security	security.samsungmobile.com text/html	MISC security.samsungmobile.com/securityUpdate.smsb?year=2021&month=5

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

An improper input validation vulnerability in sdfffd_parse_chunk_PROP() in libsdffextractor library prior to SMR MAY-...

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	11.0	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:11.0:*****:						
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)
 @CVEreport	CVE-2021-25385 : An improper input validation vulnerability in sdfffd_parse_chunk_PROP in libsdffextractor librar... twitter.com/i/web/status/1...	2021-06-11 15:05:32

[← Previous ID](#)

[Next ID →](#)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)