



CVE-2021-30020

Published on: 04/19/2021 12:00:00 AM UTC

Last Modified on: 04/21/2021 07:02:00 PM UTC

CVE-2021-30020

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

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

In the function `gf_hevc_read_pps_bs_internal` function in `media_tools/av_parsers.c` in GPAC 1.0.1 there is a loop, which with crafted file, `pps->num_tile_columns` may be larger than `sizeof(pps->column_width)`, which results in a heap overflow in the loop.

CVE-2021-30020 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
add safety in avc/hevc/vvc sps/pps/vps ID check - cf #1720 #1721 #1722 · gpac/gpac@51cdb67 · GitHub	github.com text/html	MISC github.com/gpac/gpac/commit/51cdb67ff7c5f1242ac58c5aa603ceaf1793b788
A heap overflow in function	github.com	MISC github.com/gpac/gpac/issues/1722

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.

Related QID Numbers

179453 Debian Security Update for gpac (CVE-2021-30020)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gpac	Gpac	1.0.1	All	All	All
cpe:2.3:a:gpac:gpac:1.0.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE