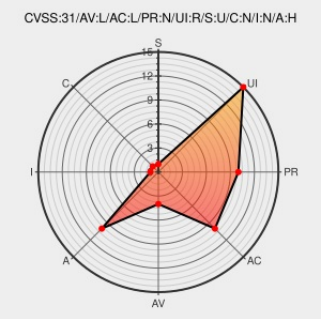
CVE-2021-30019

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

Last Modified on: 04/21/2021 07:01:00 PM UTC

CVE-2021-30019

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



Certain versions of Gpac from Gpac contain the following vulnerability:

In the adts_dmx_process function in filters/reframe_adts.c in GPAC 1.0.1, a crafted file may cause ctx->hdr.frame_size to be smaller than ctx->hdr.hdr_size, resulting in size to be a negative number and a heap overflow in the memcpy.

CVE-2021-30019 has been assigned by 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
fixed potential crash in adts reframer with broken streams - cf #1723 · gpac/gpac@22774aa · GitHub	github.com text/html	MISC github.com/gpac/gpac/commit/22774aa9e62f586319c8f107f5bae950fed900bc
A integer (heap) overflow in function	github.com	MISC github.com/gpac/gpac/issues/1723

adts_dmx_process · Issue #1723 · gpac/gpac text/html
· GitHub

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

179468 Debian Security Update for gpac (CVE-2021-30019)

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

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report