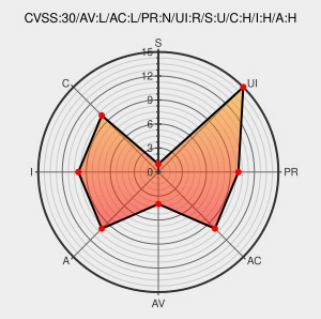
CVE-2018-20762

Published on: 02/06/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:36 PM UTC

CVE-2018-20762

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

GPAC version 0.7.1 and earlier has a buffer overflow vulnerability in the cat_multiple_files function in applications/mp4box/fileimport.c when MP4Box is used for a local directory containing crafted filenames.

CVE-2018-20762 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 1693-1] gpac security update	Mailing List, Third Party Advisory, lists.debian.org, text/html	MLIST [debian-lts-announce] 20190227 [SECURITY] [DLA 1693-1] gpac security update

USN-3926-1: GPAC vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3926-1
buffer overflow issue 4# · Issue #1187 · gpac/gpac · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/gpac/gpac/issues/1187
fix some overflows due to strcpy · gpac/gpac@35ab447 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/gpac/gpac/commit/35ab4475a7df9b2a4bcab235e379c0c3ec543658

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Gpac Project	Gpac	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:a:gpac_project:gpac:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→