



# GPAC SRT Subtitle Import text\_to\_bifs.c gf\_text\_import\_srt\_bifs out-of-bounds write

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-1418
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-01-26 04:16:10 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	A security vulnerability has been detected in GPAC up to 2.4.0. This affects the function gf_text_import_srt_bifs of the file s

## Risk And Classification

**Primary CVSS:** v4.0 1.9 LOW from cna@vulldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-119 | CWE-787 | CWE-787 Out-of-bounds Write | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	1.9	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vulldb.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	5.3	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vulldb.com	Secondary	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gpac	Gpac	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	GPAC	affected 2.0	Not specified
CNA	Na	GPAC	affected 2.1	Not specified
CNA	Na	GPAC	affected 2.2	Not specified
CNA	Na	GPAC	affected 2.3	Not specified
CNA	Na	GPAC	affected 2.4.0	Not specified

### References

Reference	Source	Link	Tags
vuldb.com	cna@vuldb.com	<a href="#">vuldb.com</a>	Permissions Required
github.com/enocknt/gpac/commit/10c73b82cf0e367383d091db38566a0e4fe71772	cna@vuldb.com	<a href="#">github.com</a>	Patch
github.com/gpac/gpac/issues/3425	cna@vuldb.com	<a href="#">github.com</a>	Exploit, Issue Tracking
github.com/gpac/gpac	cna@vuldb.com	<a href="#">github.com</a>	
github.com/gpac/gpac/issues/3425	cna@vuldb.com	<a href="#">github.com</a>	Exploit, Issue Tracking
vuldb.com	cna@vuldb.com	<a href="#">vuldb.com</a>	Third Party Advisory, \
vuldb.com	cna@vuldb.com	<a href="#">vuldb.com</a>	Third Party Advisory, \
CVE Program record	CVE ORG	<a href="#">www.cve.org</a>	canonical

CVE Program Record

NVD vulnerability detail

CVE-CNA

NVD

[www.cve.org](http://www.cve.org)

[nvd.nist.gov](http://nvd.nist.gov)

canonical, analysis

---

Vendor Comments And Credit

Discovery Credit

**CNA:** Kery Qi (VuIDB User) (en)

---

Additional Advisory Data

Source	Time	Event
CNA	2026-01-25T00:00:00.000Z	Advisory disclosed
CNA	2026-01-25T01:00:00.000Z	VuIDB entry created
CNA	2026-01-29T02:01:26.000Z	VuIDB entry last update

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)