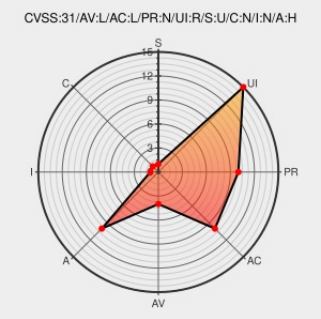
CVE-2020-21684

Published on: 08/10/2021 12:00:00 AM UTC

Last Modified on: 12/07/2022 01:55:00 AM UTC

CVE-2020-21684

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



Certain versions of Fig2dev from Fig2dev Project contain the following vulnerability:

A global buffer overflow in the put_font in genpict2e.c of fig2dev 3.2.7b allows attackers to cause a denial of service (DOS) via converting a xfig file into pict2e format.

CVE-2020-21684 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
Xfig / Tickets / #75 global-buffer-overflow in put_font at genpict2e.c:2229	sourceforge.net text/html	MISC sourceforge.net/p/mcj/tickets/75/

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

180693 Debian Security Update for fig2dev (CVE-2020-21684)

355831 Amazon Linux Security Advisory for transfig : ALAS-2023-1807

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fig2dev Project	Fig2dev	3.2.7	beta	All	All
Application	Fig2dev Project	Fig2dev	3.2.7b	All	All	All

cpe:2.3:a:fig2dev_project:fig2dev:3.2.7:beta:*:*:*:*:*:*:

cpe:2.3:a:fig2dev_project:fig2dev:3.2.7b:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-21684 : A global buffer overflow in the put_font in genpict2e.c of fig2dev 3.2.7b allows attackers to caus… twitter.com/i/web/status/1…	2021-08-10 21:11:01
@WesUncensored	New vulnerability on the NVD: CVE-2020-21684 ift.tt/3iA1vEw	2021-08-10 22:33:17

← Previous ID

Next ID→