



CVE-2021-30499

Published on: 05/26/2021 12:00:00 AM UTC

Last Modified on: 02/12/2023 10:15:00 PM UTC

CVE-2021-30499

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

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

A flaw was found in libcac. A buffer overflow of export.c in function export_troff might lead to memory corruption and other potential consequences.

CVE-2021-30499 has been assigned by secalert@redhat.com 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] Fedora 34 Update: libcaca-0.99-0.59.beta20.fc34	lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/PC7EGOEQ5C4OD66ZUJJIIYEXBTZOCMZ/

- package-
announce -
Fedora Mailing-
Lists

[SECURITY]

Fedora 35

Update: libcaca-
0.99-

0.59.beta20.fc35

- package-
announce -
Fedora Mailing-
Lists

lists.fedoraproject.org

text/html



MISC [lists.fedoraproject.org/archives/list/package-
announce%40lists.fedoraproject.org/message/6WFGYICNTMNDNMDDUV4G2RYFB5HNJCOV/](https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/6WFGYICNTMNDNMDDUV4G2RYFB5HNJCOV/)

[SECURITY]

Fedora 36

Update: libcaca-
0.99-

0.59.beta20.fc36

- package-
announce -
Fedora Mailing-
Lists

lists.fedoraproject.org

text/html



MISC [lists.fedoraproject.org/archives/list/package-
announce%40lists.fedoraproject.org/message/ZSBCRN6EGQJUVOSD4OEEQ6XORHEM2CUL/](https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ZSBCRN6EGQJUVOSD4OEEQ6XORHEM2CUL/)

1948679 – (CVE-
2021-30499)

CVE-2021-30499

libcaca: Global
buffer overflow of
export.c in
function
export_troff

bugzilla.redhat.com

text/html



MISC bugzilla.redhat.com/show_bug.cgi?id=1948679

[Security] global-
buffer-overflow of
export.c in
function

export_troff ·

Issue #54 ·

cacalabs/libcaca

· GitHub

github.com

text/html



MISC github.com/cacalabs/libcaca/issues/54

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

[182830](#) Debian Security Update for libcaca (CVE-2021-30499)

[198545](#) Ubuntu Security Notification for libcaca Vulnerabilities (USN-5119-1)

[282517](#) Fedora Security Update for libcaca (FEDORA-2022-fc6b53e7a2)

[282518](#) Fedora Security Update for libcaca (FEDORA-2022-e3b9986722)

[502107](#) Alpine Linux Security Update for libcaca

[751834](#) SUSE Enterprise Linux Security Update for libcaca (SUSE-SU-2022:0754-1)

[751842](#) SUSE Enterprise Linux Security Update for libcaca (SUSE-SU-2022:0769-1)

- 751848 OpenSUSE Security Update for libcacaca (openSUSE-SU-2022:0769-1)
- 751866 SUSE Enterprise Linux Security Update for libcacaca (SUSE-SU-2022:0820-1)
- 753261 SUSE Enterprise Linux Security Update for libcacaca (SUSE-SU-2022:14909-1)

Exploit/POC from Github

A flaw was found in libcacaca. A buffer overflow of export.c in function export_troff might lead to memory corruption a...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Libcacaca Project	Libcacaca	-	All	All	All
cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:						
cpe:2.3:a:libcacaca_project:libcacaca:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-30499 : A flaw was found in libcacaca. A buffer overflow of export.c in function export_troff might lead to... twitter.com/i/web/status/1...	2021-05-27 00:02:45
 /r/netcve	CVE-2021-30499	2021-05-27 00:41:29

← Previous ID

Next ID →

