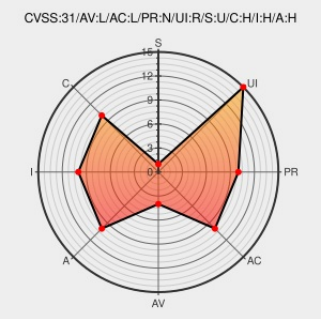
# CVE-2021-30498

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

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

## CVE-2021-30498

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




Certain versions of Fedora from Fedoraproject contain the following vulnerability:

A flaw was found in libcaca. A heap buffer overflow in export.c in function export_tga might lead to memory corruption and other potential consequences.

CVE-2021-30498 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/PC7EGOEQ5C4OD66ZUJJIIYEXBTZOCMZX/ |

| | | |
|---|---|---|
| - 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/ |
| [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/ |
| 1948675 – (CVE-2021-30498) CVE-2021-30498 libcaca: Heap buffer overflow of export.c in function export_tga | bugzilla.redhat.com text/html | MISC bugzilla.redhat.com/show_bug.cgi?id=1948675 |
| [ Security] heap-buffer-overflow of export.c in function export_tga · Issue #53 · cacalabs/libcaca · GitHub | github.com text/html | MISC github.com/cacalabs/libcaca/issues/53 |



## Related QID Numbers

184283 Debian Security Update for libcaca (CVE-2021-30498)

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 libcaca (openSUSE-SU-2022:0769-1)

751866 SUSE Enterprise Linux Security Update for libcaca (SUSE-SU-2022:0820-1)

753261 SUSE Enterprise Linux Security Update for libcaca (SUSE-SU-2022:14909-1)

## Exploit/POC from Github

PoC for exploiting CVE-2021-30498

## 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 | Libcaca Project | Libcaca | - | All | All | All |
| Application | Libcaca Project | Libcaca | 0.99 | beta14 | All | All |
| Application | Libcaca Project | Libcaca | 0.99 | beta15 | All | All |
| Application | Libcaca Project | Libcaca | 0.99 | beta16 | All | All |
| Application | Libcaca Project | Libcaca | 0.99 | beta17 | All | All |
| Application | Libcaca Project | Libcaca | 0.99 | beta18 | All | All |
| Application | Libcaca Project | Libcaca | 0.99 | beta19 | 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:libcaca_project:libcaca:-:*:*:*:*:*:*:*:

cpe:2.3:a:libcaca_project:libcaca:0.99:beta14:*:*:*:*:*:*:

cpe:2.3:a:libcaca_project:libcaca:0.99:beta15:*:*:*:*:*:*:

cpe:2.3:a:libcaca_project:libcaca:0.99:beta16:*:*:*:*:*:*:

cpe:2.3:a:libcaca_project:libcaca:0.99:beta17:*:*:*:*:*:*:

cpe:2.3:a:libcaca_project:libcaca:0.99:beta18:*:*:*:*:*:*:

cpe:2.3:a:libcaca_project:libcaca:0.99:beta19:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
| --- | --- | --- |
| @CVEreport | CVE-2021-30498 : A flaw was found in libcaca. A heap buffer overflow in export.c in function export_tga might lead… twitter.com/i/web/status/1… | 2021-05-26 22:09:17 |
| /r/netcve | CVE-2021-30498 | 2021-05-26 22:41:45 |

← Previous ID

Next ID→