

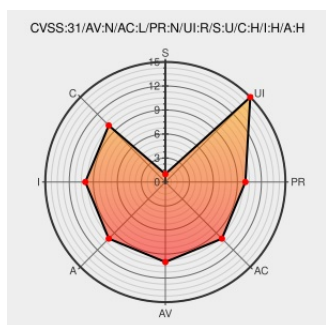


CVE-2018-20549

Published on: 12/27/2018 12:00:00 AM UTC

Last Modified on: 04/15/2022 04:11:00 PM UTC

CVE-2018-20549

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

There is an illegal WRITE memory access at caca/file.c (function caca_file_read) in libcaca 0.99.beta19.

CVE-2018-20549 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-e3b9986722
[SECURITY] [DLA 1631-1] libcaca security update	Mailing List Third Party Advisory	MLIST [debian-lts-announce] 20190109 [SECURITY] [DLA 1631-1] libcaca security

	lists.debian.org text/html	update
[SECURITY] Fedora 35 Update: libcaca-0.99-0.59.beta20.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2022-fc6b53e7a2
[security-announce] openSUSE-SU-2019:1144-1: moderate: Security update f	lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:1144
1652628 – There is an illegal WRITE memory access at caca/file.c:207 (function:caca_file_read)in libcaca latest version.	Exploit Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1652628
USN-3860-1: libcaca vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3860-1
[SECURITY] Fedora 36 Update: libcaca-0.99-0.59.beta20.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2022-3d291845d8
USN-3860-2: libcaca vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3860-2

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

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

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

[501032](#) Alpine Linux Security Update for libcaca

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	18.04	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
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	0.99	beta19	All	All
Application	Libcaca Project	Libcaca	0.99	beta19	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:						
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:12.04:*:*:*:esm:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:						
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: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:0.99:beta19:*:*:*:*:*:						

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

cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)