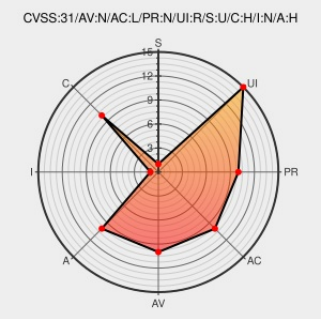
CVE-2018-20546

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

Last Modified on: 11/07/2023 02:56:00 AM UTC

CVE-2018-20546

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

There is an illegal READ memory access at caca/dither.c (function get_rgba_default) in libcaca 0.99.beta19 for the default bpp case.

CVE-2018-20546 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	HIGH

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	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 lists.debian.org text/html	MLIST [debian-lts-announce] 20190109 [SECURITY] [DLA 1631-1] libcaca security 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
1652622 – There is an illegal READ memory access at caca/dither.c:1347 (function:get_rgba_default)in libcaca latest version.	Exploit Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1652622
[security-announce] openSUSE-SU-2019:1144-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2019:1144
[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
dither: fix integer multiplication overflow that caused crashes. · cacalabs/libcaca@1022d97 · GitHub	github.com text/html	MISC github.com/cacalabs/libcaca/commit/1022d97496c7899e8641515af363381b31ae2f05
USN-3860-1: libcaca vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3860-1
USN-3860-2: libcaca vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3860-2
CVE-2018-20546 · Issue #38 · cacalabs/libcaca · GitHub	github.com text/html	MISC github.com/cacalabs/libcaca/issues/38

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

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	18.10	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→