

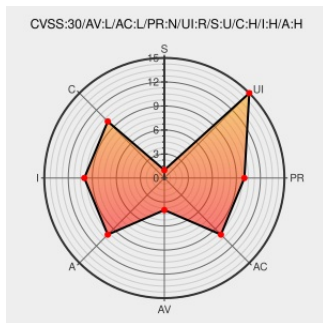


CVE-2017-7961

Published on: 04/19/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:40 PM UTC

CVE-2017-7961

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

Certain versions of [Libcroco](#) from [Gnome](#) contain the following vulnerability:

**** DISPUTED **** The `cr_tknzr_parse_rgb` function in `cr-tknzr.c` in `libcroco` 0.6.11 and 0.6.12 has an "outside the range of representable values of type long" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted CSS file. NOTE:

third-party analysis reports "This is not a security issue in my view. The conversion surely is truncating the double into a long value, but there is no impact as the value is one of the RGB components."

CVE-2017-7961 has been assigned by [M](#) [cve@mitre.org](#) 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
-------------	------	------

Bug 1034482 – VUL-1: CVE-2017-7961: libcroco: undefined behavior (tknzs: support only max long rgb values)	Issue Tracking Patch Third Party Advisory bugzilla.suse.com text/html	 MISC bugzilla.suse.com/show_bug.cgi?id=1034482
oss-security - Re: libcroco: heap overflow and undefined behavior	Mailing List Patch Third Party Advisory openwall.com text/html	 MISC openwall.com/lists/oss-security/2017/04/24/2
libcroco: heap overflow and undefined behavior agostino's blog	Exploit Patch Third Party Advisory blogs.gentoo.org text/html	 MISC blogs.gentoo.org/ago/2017/04/17/libcroco-heap-overflow-and-undefined-behavior/
[security-announce] openSUSE-SU-2019:1575-1: moderate: Security update f	lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:1575
tknzs: support only max long rgb values (9ad72875) · Commits · GNOME / libcroco · GitLab	Issue Tracking Patch Third Party Advisory git.gnome.org text/html	 MISC git.gnome.org/browse/libcroco/commit?id=9ad72875e9f08e4c519ef63d44cbbd94aa9504f7
libcroco: Multiple vulnerabilities (GLSA 201707-13) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201707-13

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

710468 Gentoo Linux libcroco Multiple Vulnerabilities (GLSA 201707-13)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Libcroco	0.6.11	All	All	All
Application	Gnome	Libcroco	0.6.12	All	All	All
Application	Gnome	Libcroco	0.6.11	All	All	All
Application	Gnome	Libcroco	0.6.12	All	All	All
cpe:2.3:a:gnome:libcroco:0.6.11:*****:						
cpe:2.3:a:gnome:libcroco:0.6.12:*****:						
cpe:2.3:a:gnome:libcroco:0.6.11:*****:						
cpe:2.3:a:gnome:libcroco:0.6.12:*****:						

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](#)