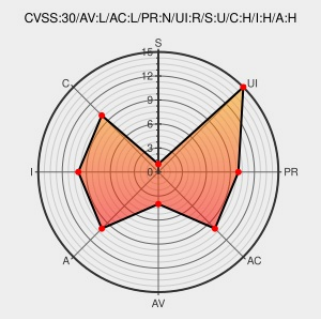
# CVE-2017-7961

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 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 (tknzr: support only max long rgb values) | Issue Tracking<br>Patch<br>Third Party Advisory<br>bugzilla.suse.com<br>text/html | MISC bugzilla.suse.com/show_bug.cgi?id=1034482 |
| oss-security - Re: libcroco: heap overflow and undefined behavior | Mailing List<br>Patch<br>Third Party Advisory<br>openwall.com<br>text/html | MISC openwall.com/lists/oss-security/2017/04/24/2 |
| libcroco: heap overflow and undefined behavior \| agostino's blog | Exploit<br>Patch<br>Third Party Advisory<br>blogs.gentoo.org<br>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<br>text/html | SUSE openSUSE-SU-2019:1575 |
| tknzr: support only max long rgb values (9ad72875) · Commits · GNOME / libcroco · GitLab | Issue Tracking<br>Patch<br>Third Party Advisory<br>git.gnome.org<br>text/html | MISC git.gnome.org/browse/libcroco/commit/?id=9ad72875e9f08e4c519ef63d44cdbd94aa9504f7 |
| libcroco: Multiple vulnerabilities (GLSA 201707-13) — Gentoo security | Third Party Advisory<br>security.gentoo.org<br>text/html | GENTOO GLSA-201707-13 |



## 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 and Source URL Uptime Status status.cve.report**