



# CVE-2017-7960

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

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

## CVE-2017-7960

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

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

The `cr_input_new_from_uri` function in `cr-input.c` in `libcroco` 0.6.11 and 0.6.12 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted CSS file.

CVE-2017-7960 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                      | Tags                                                                                                                                                      | Link                                                                                                |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| libcroco: heap overflow and undefined behavior   agostino's blog | <a href="#">Exploit</a><br><a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">blogs.gentoo.org</a><br><a href="#">text/html</a> | <a href="#">MISC blogs.gentoo.org/ago/2017/04/17/libcroco-heap-overflow-and-undefined-behavior/</a> |

input: check end of input before reading a byte (898e3a8c) · Commits · GNOME / libcroco · GitLab

Patch

Third Party Advisory

git.gnome.org

text/html

MISC

git.gnome.org/browse/libcroco/commit/?id=898e3a8c8c0314d2e6b106809a8e3e93cf9d4394

[security-announce] openSUSE-SU-2019:1575-1: moderate: Security update f

lists.opensuse.org

text/html

SUSE

openSUSE-SU-2019:1575

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](mailto: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