



CVE-2020-6609

Published on: 01/08/2020 12:00:00 AM UTC

Last Modified on: 09/12/2022 06:45:00 PM UTC

CVE-2020-6609

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Libredwg](#) from [Gnu](#) contain the following vulnerability:

GNU LibreDWG 0.9.3.2564 has a heap-based buffer over-read in `read_pages_map` in `decode_r2007.c`.

CVE-2020-6609 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
Several bugs found by fuzzing · Issue #179 · LibreDWG/libredwg · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/LibreDWG/libredwg/issues/179#issue-544834443

[security-announce] openSUSE-SU-2020:0115-1: moderate: Security update f

lists.opensuse.org
text/html

 SUSE openSUSE-SU-2020:0115

[security-announce] openSUSE-SU-2020:0096-1: moderate: Security update f

lists.opensuse.org
text/html

 SUSE openSUSE-SU-2020:0096

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Libredwg	0.9.3.2564	All	All	All
Application	Gnu	Libredwg	0.9.3.2564	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

cpe:2.3:a:gnu:libredwg:0.9.3.2564:*:*:*:*:*:

cpe:2.3:a:gnu:libredwg:0.9.3.2564:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID→