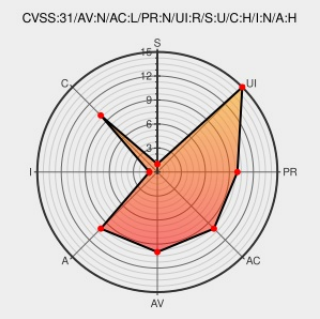
CVE-2019-20910

Published on: 07/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:51 PM UTC

CVE-2019-20910

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



Certain versions of Libredwg from Gnu contain the following vulnerability:

An issue was discovered in GNU LibreDWG through 0.9.3. Crafted input will lead to a heap-based buffer over-read in decode_R13_R2000 in decode.c, a different vulnerability than CVE-2019-20011.

CVE-2019-20910 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
add DEBUGGING_CLASS_CPP · LibreDWG/libredwg@f878ba6 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/LibreDWG/libredwg/commit/f878ba67b638f0d5050b6dba61b9737f64fc53de

Several bugs need to be fixed. · Issue #178 · LibreDWG/libredwg · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/LibreDWG/libredwg/issues/178

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	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→