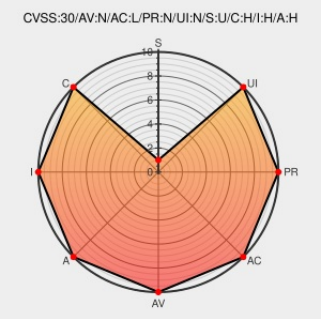
CVE-2017-9433

Published on: 06/04/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:57 PM UTC

CVE-2017-9433

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



Certain versions of Libmwaw from Libmwaw Project contain the following vulnerability:

Document Liberation Project libmwaw before 2017-04-08 has an out-of-bounds write caused by a heap-based buffer overflow related to the MsWrd1Parser::readFootnoteCorrespondance function in lib/MsWrd1Parser.cxx.

CVE-2017-9433 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3875-1 libmwaw	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3875
libmwaw / Libmwaw / Commit [68b3b7]	Patch	MISC

	Third Party Advisory sourceforge.net text/html	sourceforge.net/p/libmwaw/libmwaw/ci/68b3b74569881248bfb6cbb426
1037 - dlplibs: Heap-buffer-overflow in MsWrd1Parser::readFootnoteCorrespondance - oss-fuzz - Monorail	Issue Tracking Third Party Advisory VDB Entry bugs.chromium.org text/html	MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=1037

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	Libmwaw Project	Libmwaw	All	All	All	All

cpe:2.3:a:libmwaw_project:libmwaw:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→