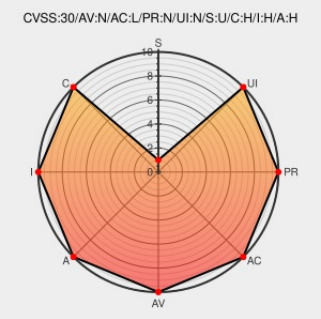
CVE-2019-5041

Published on: 08/21/2019 12:00:00 AM UTC

Last Modified on: 06/27/2022 05:28:00 PM UTC

CVE-2019-5041

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



Certain versions of Aspose.words from Aspose contain the following vulnerability:

An exploitable Stack Based Buffer Overflow vulnerability exists in the EnumMetaInfo function of Aspose Aspose.Words library, version 18.11.0.0. A specially crafted doc file can cause a stack-based buffer overflow, resulting in remote code execution. An attacker needs to provide a malformed file to the victim to trigger this vulnerability.

CVE-2019-5041 has been assigned by talos-cna@cisco.com 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
TALOS-2019-0805 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Third Party Advisory www.talosintelligence.com application/octet-stream	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2019-0805

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	Aspose	Aspose.words	18.11.0.0	All	All	All
Application	Aspose	Aspose.words	18.11.0.0	All	All	All

cpe:2.3:a:aspose:aspose.words:18.11.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:aspose:aspose.words:18.11.0.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→