



CVE-2021-25832

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-25832
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-01 16:15:00 UTC
Updated	2021-03-15 19:53:00 UTC
Description	A heap buffer overflow vulnerability inside of BMP image processing was found at [core] module of ONLYOFFICE Document Server

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Onlyoffice	Document Server	All	All	All	All

References

Reference
GitHub - ONLYOFFICE/core: Server core components which are a part of ONLYOFFICE Document Server
core/BinaryFileReaderWriter.cpp at v6.0.1.15 · ONLYOFFICE/core · GitHub
core/ximabmp.cpp at v6.0.1.15 · ONLYOFFICE/core · GitHub
GitHub - ONLYOFFICE/DocumentServer: ONLYOFFICE Docs is a free collaborative online office suite comprising viewers and editors for text documents
core/BinaryFileReaderWriter.cpp at v6.0.1.15 · ONLYOFFICE/core · GitHub
core/ximabmp.cpp at v6.0.1.15 · ONLYOFFICE/core · GitHub
poc_exploits/ONLYOFFICE/CVE-2021-25832 at master · merrychap/poc_exploits · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)