



CVE-2021-26259

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

Summary

CVE	CVE-2021-26259
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-03 23:15:00 UTC
Updated	2023-11-07 03:31:00 UTC
Description	A flaw was found in htmldoc in v1.9.12. Heap buffer overflow in render_table_row(), in ps-pdf.cxx may lead to arbitrary code

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Htmldoc Project	Htmldoc	1.9.12	All	All	All

References

Reference	Source
Fix a crash bug with bogus table attributes (Issue #417) · michaelrsweet/htmldoc@0ddab26 · GitHub	MISC
AddressSanitizer: heap-buffer-overflow on render_table_row() ps-pdf.cxx:6123:34 · Issue #417 · michaelrsweet/htmldoc · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [178664](#) Debian Security Update for htmldoc (DSA 4928-1)
- [178690](#) Debian Security Update for htmldoc (DLA 2700-1)
- [180460](#) Debian Security Update for htmldoc (CVE-2021-26259)

© [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](#)