



CVE-2021-23158

Published on: Not Yet Published

Last Modified on: 02/12/2023 10:10:56 PM UTC

CVE-2021-23158

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [HtmlDoc](#) from [HtmlDoc Project](#) contain the following vulnerability:

A flaw was found in htmldoc in v1.9.12. Double-free in function `pspdf_export()`, in `ps-pdf.cxx` may result in a write-what-where condition, allowing an attacker to execute arbitrary code and denial of service.

CVE-2021-23158 has been assigned by secalert@redhat.com 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
AddressSanitizer: double-free in function <code>pspdf_export</code> <code>ps-pdf.cxx</code> :945:7 · Issue #414 · michaelrsweet/htmldoc · GitHub	github.com text/html	MISC github.com/michaelrsweet/htmldoc/issues/414

Fix JPEG error handling (Issue #415) · michaelrsweet/htmldoc@369b2ea · GitHub

[github.com](#)
[text/html](#)

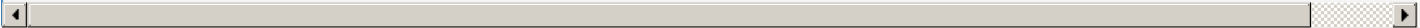
 MISC
[github.com/michaelrsweet/htmldoc/commit/369b2ea1fd0d0537ba707f20a2f047b6af](#)

1967018 – (CVE-2021-23158)
CVE-2021-23158 htmldoc:
double-free in function
pspdf_export()

[bugzilla.redhat.com](#)
[text/html](#)

 MISC [bugzilla.redhat.com/show_bug.cgi?id=1967018](#)

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.



Related QID Numbers

[178664](#) Debian Security Update for htmldoc (DSA 4928-1)

[178690](#) Debian Security Update for htmldoc (DLA 2700-1)

[180399](#) Debian Security Update for htmldoc (CVE-2021-23158)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Htmldoc Project	Htmldoc	1.9.12	All	All	All
cpe:2.3:a:htmldoc_project:htmldoc:1.9.12:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @vigilance_en	Vigil@nce #Vulnerability of htmldoc: multiple vulnerabilities. vigilance.fr/vulnerability/... Identifiers: #CVE-2021-23158... twitter.com/i/web/status/1...	2021-06-10 16:09:04
 @CVEreport	cve.report/CVE-2021-23158 A flaw was found in htmldoc in v1.9.12. Double-free in function pspdf_export ,in ps-pdf.c... twitter.com/i/web/status/1...	2022-03-16 16:18:42
 @WesUncensored	New vulnerability on the NVD: CVE-2021-23158 ift.tt/aBFw3J4	2022-03-16 16:33:14
 /r/netcve	CVE-2021-23158	2022-03-16 17:38:41

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](#).

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