



CVE-2021-23180

Published on: Not Yet Published

Last Modified on: 03/10/2022 07:27:00 PM UTC

CVE-2021-23180

[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 and before. Null pointer dereference in file_extension(), in file.c may lead to execute arbitrary code and denial of service.

CVE-2021-23180 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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
CVE-2021-23180 Ubuntu	ubuntu.com text/html	MISC ubuntu.com/security/CVE-2021-23180
Fix a crash bug with malformed URIs (Issue #418) ·	github.com text/html	MISC github.com/michaelsweet/htmldoc/commit/19c582fb32eac74b57e155cffb529377a9

1967041 – (CVE-2021-23180)
CVE-2021-23180 htmldoc: null
pointer dereference in function in
file_extension()

bugzilla.redhat.com

text/html

 [MISC bugzilla.redhat.com/show_bug.cgi?id=1967041](https://bugzilla.redhat.com/show_bug.cgi?id=1967041)

AddressSanitizer: SEGV in
file_extension file.c:337:29 ·
Issue #418 ·
michaelsweet/htmldoc · Git

github.com

text/html

 MISC github.com/michaelsweet/htmlDoc/issues/418

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)

179994 Debian Security Update for htmldoc (CVE-2021-23180)

198612 Ubuntu Security Notification for HTMLDOC Vulnerability (USN-5198-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Htmldoc Project	Htmldoc	All	All	All	All
<code>cpe:2.3:a:htmldoc_project:htmldoc:*:*:*:*:*:*</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-23180 : A flaw was found in htmldoc in v1.9.12 and before. Null pointer dereference in file_extension ,in... twitter.com/i/web/status/1...	2022-03-02 23:16:33
 /r/netcve	CVE-2021-23180	2022-03-03 00:38:49

[← Previous ID](#)

Next ID→

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](#)