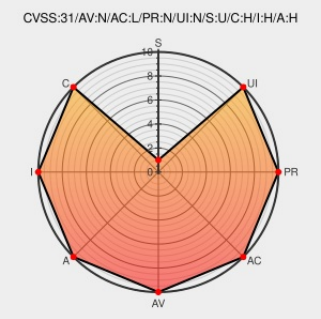
CVE-2021-23165

Published on: Not Yet Published

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

CVE-2021-23165

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 before v1.9.12. Heap buffer overflow in pspdf_prepare_outpages(), in ps-pdf.cxx may lead to execute arbitrary code and denial of service.

CVE-2021-23165 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: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Fix a number-up crash bug (Issue #413) · michaelrsweet/htmldoc@6e8a955 · GitHub	github.com text/html	MISC github.com/michaelrsweet/htmldoc/commit/6e8a95561988500b5b5ae4861b3b0cbf4

	github.com text/x-diff	MISC github.com/michaelrsweet/htmldoc/commit/6e8a95561988500b5b5ae4861b3b0cbf4
AddressSanitizer: heap-buffer-overflow in pspdf_prepare_outpages() in ps-pdf.cxx:1338:15 · Issue #413 · michaelrsweet/htmldoc · GitHub	github.com text/html	MISC github.com/michaelrsweet/htmldoc/issues/413
1967014 – (CVE-2021-23165) CVE-2021-23165 htmldoc: heap-buffer-overflow in pspdf_prepare_outpages()	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1967014

Related QID Numbers

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

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

179886 Debian Security Update for htmldoc (CVE-2021-23165)

198796 Ubuntu Security Notification for HTMLDOC Vulnerability (USN-5438-1)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:htmldoc_project:htmldoc:*:*:*:*:*:*:*:*:

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)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-23165 A flaw was found in htmldoc before v1.9.12. Heap buffer overflow… twitter.com/i/web/status/1…	2022-03-16 15:56:01
@CVEreport	cve.report/CVE-2021-23165 A flaw was found in htmldoc before v1.9.12. Heap buffer overflow in pspdf_prepare_outpages… twitter.com/i/web/status/1…	2022-03-16 16:19:05
@WesUncensored	New vulnerability on the NVD: CVE-2021-23165 ift.tt/xWhnr7i	2022-03-16 16:33:13
/r/netcve	CVE-2021-23165	2022-03-16 17:38:42

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report