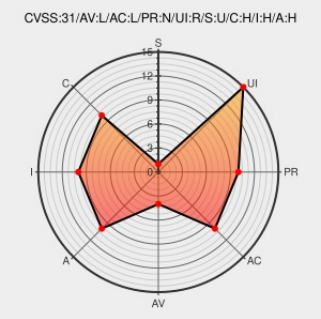
CVE-2021-43579

Published on: 11/12/2021 12:00:00 AM UTC

Last Modified on: 04/01/2022 03:20:00 PM UTC

CVE-2021-43579

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

A stack-based buffer overflow in image_load_bmp() in HTMLDOC <= 1.9.13 results in remote code execution if the victim converts an HTML document linking to a crafted BMP file.

CVE-2021-43579 has been assigned by cve@mitre.org 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
Stack Buffer Overflow with BMP files - Version 1.9.13 · Issue #456 · michaelrsweet/htmldoc · GitHub	github.com text/html	MISC github.com/michaelrsweet/htmldoc/issues/456
Comparing v1.9.12...v1.9.13 ·	github.com	MISC github.com/michaelrsweet/htmldoc/compare/v1.9.12...v1.9.13

michaelrsweet/htmldoc · GitHub	text/html	
Stack buffer overflow in image_load_bmp() · Issue #453 · michaelrsweet/htmldoc · GitHub	github.com text/html	MISC github.com/michaelrsweet/htmldoc/issues/453
Fix potential BMP stack overflow (Issue #453) · michaelrsweet/htmldoc@27d0898 · GitHub	github.com text/html	MISC github.com/michaelrsweet/htmldoc/commit/27d08989a5a567155d506ac870ae7d8cc88f
[SECURITY] [DLA 2928-1] htmldoc security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20220226 [SECURITY] [DLA 2928-1] htmldoc security update

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

179095 Debian Security Update for htmldoc (DLA 2928-1)

180550 Debian Security Update for htmldoc (CVE-2021-43579)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Htmldoc Project	Htmldoc	All	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43579 : A stack-based buffer overflow in image_load_bmp in HTMLDOC before 1.9.13 results in remote code… twitter.com/i/web/status/1…	2021-11-12 18:48:26
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-43579 Description: A stack-based buffer overflow in image_load_bmp() in… twitter.com/i/web/status/1…	2021-11-12 19:00:10

← Previous ID

Next ID→

© CVE.report 2023 |
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 registred 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