

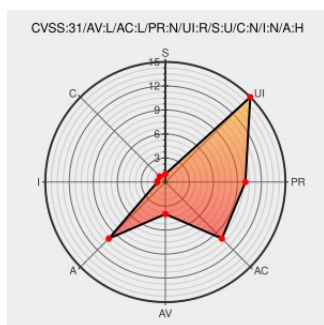


CVE-2021-40647

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2021-40647

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

Certain versions of [Man2html](#) from [Man2html Project](#) contain the following vulnerability:

In man2html 1.6g, a specific string being read in from a file will overwrite the size parameter in the top chunk of the heap. This at least causes the program to segmentation abort if the heap size parameter isn't aligned correctly. In version before GLIBC version 2.29 and aligned correctly, it allows arbitrary write anywhere in the programs

memory.

CVE-2021-40647 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
CVE-2021-40647 and CVE-2021-40648 · GitHub	gist.github.com text/html	MISC gist.github.com/untaman/cb58123fe89fc65e3984165db5d40933
No Description Provided	man2html.com	MISC man2html.com
	Inactive Link Not Archived	
Commercial Distributor & Supply Company North American	na.com text/html	MISC na.com

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

There are currently no QIDs associated with this CVE

Exploit/POC from Github

In man2html 1.6g, a specific string being read in from a file will overwrite the size parameter in the top chunk of t...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Man2html Project	Man2html	1.6g	All	All	All
cpe:2.3:a:man2html_project:man2html:1.6g:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-40647 : In man2html 1.6g, a specific string being read in from a file will overwrite the size parameter in... twitter.com/i/web/status/1...	2022-09-09 18:02:01
 /r/netcve	CVE-2021-40647	2022-09-09 18:38:52

[← 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 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](#)