



CVE-2022-26110

Published on: Not Yet Published

Last Modified on: 09/03/2022 03:34:00 AM UTC

CVE-2022-26110

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

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

An issue was discovered in HTCondor 8.8.x before 8.8.16, 9.0.x before 9.0.10, and 9.1.x before 9.6.0. When a user authenticates to an HTCondor daemon via the CLAIMTOBE method, the user can then impersonate any entity when issuing additional commands to that daemon.

CVE-2022-26110 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 2984-1] condor security update	lists.debian.org text/html	@ MLIST [debian-lts-announce] 20220419 [SECURITY] [DLA 2984-1] condor security update
HTCondor - Page not found	research.cs.wisc.edu	📁 MISC

HTCondor - Page not found

research.cs.wisc.edu

text/html

Inactive Link

Not Archived

 research.cs.wisc.edu/htcondor/security/vulnerabilities/HTCONDOR-2022-0003/

Debian -- Security Information -- DSA-5144-1 condor

www.debian.org

Deprecated Link

text/html

 [DEBIAN DSA-5144](#)

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

- [179245](#) Debian Security Update for condor (DLA 2984-1)
- [179305](#) Debian Security Update for condor (DSA 5144-1)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wisc	Htcondor	All	All	All	All
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:wisc:htcondor:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-26110 : An issue was discovered in HTCondor 8.8.x before 8.8.16, 9.0.x before 9.0.10, and 9.1.x before 9.6... twitter.com/i/web/status/1...	2022-04-06 02:03:51
 /r/netcve	CVE-2022-26110	2022-04-06 02:38:52

© [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](#)