



CVE-2019-18823

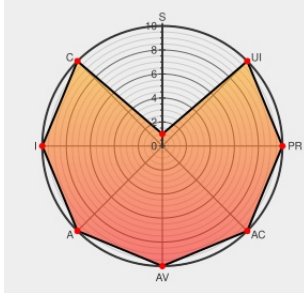
Published on: 04/27/2020 12:00:00 AM UTC

Last Modified on: 10/06/2022 05:49:00 PM UTC

CVE-2019-18823

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

HTCondor up to and including stable series 8.8.6 and development series 8.9.4 has Incorrect Access Control. It is possible to use a different authentication method to submit a job than the administrator has specified. If the administrator has configured the READ or WRITE methods to include CLAIMTOBE, then it is possible to impersonate another user to the condor_schedd. (For example to submit or remove jobs)

CVE-2019-18823 has been assigned by [M](#) cve@mitre.org 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: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
HTCondor - What's new with HTCondor?	Release Notes Vendor Advisory	MISC research.cs.wisc.edu/htcondor/new.html

	research.cs.wisc.edu text/html	
HTCONDOR-2020-0004	Vendor Advisory research.cs.wisc.edu text/html	 MISC research.cs.wisc.edu/htcondor/security/vulnerabilities/HTCONDOR-2020-0004.html
[SECURITY] Fedora 32 Update: condor-8.8.8-1.fc32 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-fb5af97476
HTCONDOR-2020-0002	Mitigation Vendor Advisory research.cs.wisc.edu text/html	 MISC research.cs.wisc.edu/htcondor/security/vulnerabilities/HTCONDOR-2020-0002.html
HTCondor - Home	Product research.cs.wisc.edu text/html	 MISC research.cs.wisc.edu/htcondor/
HTCONDOR-2020-0003	Mitigation Vendor Advisory research.cs.wisc.edu text/html	 CONFIRM research.cs.wisc.edu/htcondor/security/vulnerabilities/HTCONDOR-2020-0003.html
[SECURITY] [DLA 2724-1] condor security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20210801 [SECURITY] [DLA 2724-1] condor security update
HTCONDOR-2020-0001	Mitigation Vendor Advisory research.cs.wisc.edu text/html	 MISC research.cs.wisc.edu/htcondor/security/vulnerabilities/HTCONDOR-2020-0001.html
[SECURITY] Fedora 31 Update: condor-8.8.8-1.fc31 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-f9a598f815
Debian -- Security Information -- DSA-5144-1 condor	www.debian.org Deprecated Link text/html	 DEBIAN DSA-5144
[SECURITY] Fedora 30 Update: condor-8.8.8-1.fc30 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-ae934f6790
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

[178733](#) Debian Security Update for condor (DLA 2724-1)

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating	Debian	Debian Linux	10.0	All	All	All

System						
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Wisc	Htcondor	All	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:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:						
cpe:2.3:a:wisc:htcondor:*:*:*:*:*:						
cpe:2.3:a:wisc:htcondor:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← Previous ID Next ID →		

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](#)