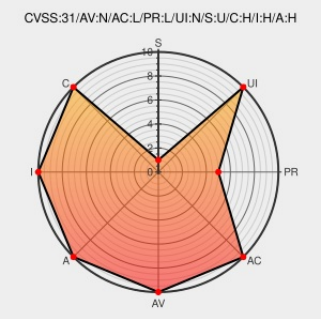
CVE-2012-3490

Published on: 01/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:17 PM UTC

CVE-2012-3490

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



Certain versions of Htcondor from Wisc contain the following vulnerability:

The (1) my_popenv_impl and (2) my_spawnv functions in src/condor_utils/my_popen.cpp and the (3) systemCommand function in condor_vm-gahp/vmgahp_common.cpp in Condor 7.6.x before 7.6.10 and 7.8.x before 7.8.4 does not properly check the return value of setuid calls, which might cause a subprocess to be created with root privileges and allow remote attackers to gain privileges via unspecified vectors.

CVE-2012-3490 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Condor** - **Condor** version **7.6.x before 7.6.10 and 7.8.x before 7.8.4**

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: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

848212 – (CVE-2012-3490) CVE-2012-3490 condor: does not check return value of setuid and similar calls, exploitable via VMware support	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=CVE-2012-3490
9.3 Stable Release Series 7.8	Release Notes Third Party Advisory research.cs.wisc.edu text/html	MISC research.cs.wisc.edu/condor/manual/v7.8/9_3Stable_Release.html
oss-security - Notification of upstream Condor security fixes	Mailing List Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2012/09/20/9
8.3 Stable Release Series 7.6	Release Notes Third Party Advisory research.cs.wisc.edu text/html	MISC research.cs.wisc.edu/condor/manual/v7.6/8_3Stable_Release.html
HTCondor Git - condor.git/commitdiff	Patch Third Party Advisory condor-git.cs.wisc.edu text/xml	MISC condor-git.cs.wisc.edu/?p=condor.git;a=commitdiff;h=94e84ce4

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wisc	Htcondor	All	All	All	All
Application	Wisc	Htcondor	All	All	All	All

cpe:2.3:a:wisc:htcondor:*:*:*:*:*:*:*:*:

cpe:2.3:a:wisc:htcondor:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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