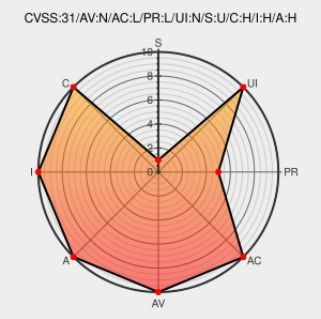
CVE-2014-8126

Published on: 01/31/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:51 PM UTC

CVE-2014-8126

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



Certain versions of Htcondor from Wisc contain the following vulnerability:

The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.

CVE-2014-8126 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **HTCondor** - **HTCondor** version **before 8.2.6**

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
[HTCondor-users] SECURITY: Addressing a problem in mailx	Vendor Advisory www-auth.cs.wisc.edu text/html	MISC www-auth.cs.wisc.edu/lists/htcondor-users/2015-January/msg00034.shtml

Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC rhn.redhat.com/errata/RHSA-2015-0036.html
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC rhn.redhat.com/errata/RHSA-2015-0035.html
1169800 – (CVE-2014-8126) CVE-2014-8126 condor: mailx invocation enables code execution as condor user	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1169800

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→