

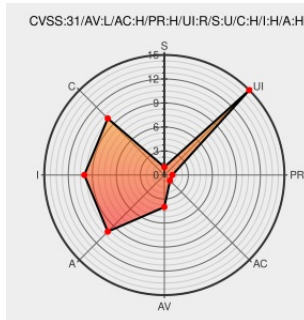


CVE-2020-10737

Published on: 05/26/2020 12:00:00 AM UTC

Last Modified on: 12/03/2022 02:26:00 AM UTC

CVE-2020-10737

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

Certain versions of [Oddjob](#) from [Redhat](#) contain the following vulnerability:

A race condition was found in the mkhomedir tool shipped with the oddjob package in versions before 0.34.5 and 0.34.6 wherein, during the home creation, mkhomedir copies the /etc/skel directory into the newly created home and changes its ownership to the home's user without properly checking the homedir path. This flaw allows an

attacker to leverage this issue by creating a symlink point to a target folder, which then has its ownership transferred to the new home directory's unprivileged user.

CVE-2020-10737 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Red Hat** - **oddjob** version **before 0.34.5**

Affected Vendor/Software: **Red Hat** - **oddjob** version **before 0.34.6**

CVSS3 Score: **6.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **3.7 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Commit - oddjob - 10b8aaa1564b723a005b53acc069df71313f4cac - Pagure.io	Patch Third Party Advisory pagure.io text/html	CONFIRM pagure.io/oddjob/c/10b8aaa1564b723a005b53acc069df71313f4cac?branch
1833042 – (CVE-2020-10737) CVE-2020-10737 oddjob: race condition in oddjob_selinux_mkdir function in mkhomedir.c can lead to symlink attack	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10737

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

377558 Alibaba Cloud Linux Security Update for oddjob (ALINUX3-SA-2022:0053)

940421 AlmaLinux Security Update for oddjob (ALSA-2020:4687)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Oddjob	All	All	All	All
Application	Redhat	Oddjob	All	All	All	All

cpe:2.3:a:redhat:oddjob:*****:

cpe:2.3:a:redhat:oddjob:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID→