

Bug 2060217 (CVE-2022-0851) - CVE-2022-0851 convert2rhel: Activation key passed via command line by code

Keywords:

Status: CLOSED ERRATA

Alias: CVE-2022-0851

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2060659 2060660 2119838

Blocks: 2054854

TreeView+ [depends on](#) / [blocked](#)

Reported: 2022-03-03 01:07 UTC by Todd Cullum

Modified: 2022-09-23 19:42 UTC ([History](#))

CC List: 3 users ([show](#))

Fixed In Version:

Doc Type: If docs needed, set a value

Doc Text: There is a flaw in convert2rhel. When the --activationkey option is used with convert2rhel, the activation key is subsequently passed to subscription-manager via the command line, which could allow unauthorized users locally on the machine to view the activation key via the process command line via e.g. htop or ps. The specific impact varies upon the subscription, but generally this would allow an attacker to register systems purchased by the victim until discovered; a form of fraud. This could occur regardless of how the activation key is supplied to convert2rhel because it involves how convert2rhel provides it to subscription-manager.

Clone Of:

Environment:

Last Closed: 2022-09-03 11:55:45 UTC

Attachments (Terms of Use)
Add an attachment (proposed patch, testcase, etc.)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2022:6266	0	None	None	None	2022-08-31 12:58:45 UTC

Red Hat Product Errata	RHSA-2022:6268	0	None	None	None	2022-08-31 13:00:17 UTC
Red Hat Product Errata	RHSA-2022:6269	0	None	None	None	2022-08-31 13:01:55 UTC

Todd Cullum 2022-03-03 01:07:28 UTC

[Description](#)



In convert2rhel's subscription.py file, code to register a system passes the activation key via the commandline. This could result in disclosure of the activation key to all users with local access to the system.

Reference:

1.
<https://github.com/oamg/convert2rhel/blob/main/convert2rhel/subscription.py#L135>

Daniel Diblik 2022-08-24 14:53:32 UTC

[Comment 4](#)

Verified by running automated tests.
 rhel-7 [ [bug 2060659](#)]
 rhel-8 [ [bug 2060660](#)]

errata-xmlrpc 2022-08-31 12:58:42 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Convert2RHEL for RHEL-6

Via RHSA-2022:6266 <https://access.redhat.com/errata/RHSA-2022:6266>

errata-xmlrpc 2022-08-31 13:00:14 UTC

[Comment 6](#)

This issue has been addressed in the following products:

Convert2RHEL for RHEL-7

Via RHSA-2022:6268 <https://access.redhat.com/errata/RHSA-2022:6268>

errata-xmlrpc 2022-08-31 13:01:53 UTC

[Comment 7](#)

This issue has been addressed in the following products:

Convert2RHEL for RHEL-8

Via RHSA-2022:6269 <https://access.redhat.com/errata/RHSA-2022:6269>

Product Security DevOps Team 2022-09-03 11:55:44 UTC

[Comment 8](#)

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

<https://access.redhat.com/security/cve/cve-2022-0851>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

