Bug 2108653 (CVE-2022-2568) - CVE-2022-2568 Ansible: Logic flaw leads to privilage escalation

Keywords: Security ×

Status: CLOSED ERRATA

Alias: CVE-2022-2568

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2108668 2108669 2108670 2108671

Blocks: 2108655

TreeView+ depends on / blocked

Reported: 2022-07-19 16:05 UTC by Vipul Nair

Modified: 2022-09-01 16:55 UTC (History)

CC List: 19 users (show)

Fixed In Version:

Doc Type: If docs needed, set a value

Doc Text: A privilege escalation flaw was found in the Ansible Automation Platform. This flaw allows a remote authenticated user with 'change user' permissions to modify the account settings of the superuser account and also remove the superuser privileges.

Clone Of:

Environment:

Last Closed: 2022-09-01 16:55:52 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-2022:6078	0	None	None	None	2022-08-16 13:20:21 UTC
Red Hat Product Errata	RHSA-2022:6079	0	None	None	None	2022-08-16 13:21:51 UTC

Vipul Nair 2022-07-19 16:05:38 UTC Description

```
User with 'change user' permissions can change any parameter
from a superuser via API but none via UI. This user can even
set the 'is_superuser' flag to false and thus remove superuser
privileges.

HTTP request:
PATCH http://localhost:5001/api/automation-hub/_ui/v1/users/1/
{"username": "admin", "is_superuser": false}

200 OK
```

errata-xmlrpc 2022-08-16 13:20:18 UTC Comment 4

```
This issue has been addressed in the following products:

  Red Hat Ansible Automation Platform 2.1 for RHEL 8

Via RHSA-2022:6078 https://access.redhat.com/errata/RHSA-
2022:6078
```

errata-xmlrpc 2022-08-16 13:21:48 UTC Comment 5

```
This issue has been addressed in the following products:

  Red Hat Ansible Automation Platform 2.2 for RHEL 8
  Red Hat Ansible Automation Platform 2.2 for RHEL 9

Via RHSA-2022:6079 https://access.redhat.com/errata/RHSA-
2022:6079
```

Product Security DevOps Team 2022-09-01 16:55:50 UTC Comment 6

```
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-2022-2568
```