Bug 1803608 (CVE-2020-1742) - CVE-2020-1742 nmstate/kubernetes-nmstate-handler: /etc/passwd is given incorrect privileges

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2020-1742
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: 1803609
Blocks: 1776664
TreeView+ depends on / blocked

Reported: 2020-02-17 02:42 UTC by Joshua Padman
Modified: 2022-08-10 14:23 UTC (History)
CC List: 5 users (show)
Fixed In Version: kubernetes-nmstate-handler-container-v2.3.0-30
Doc Type: If docs needed, set a value
Doc Text: An insecure modification vulnerability flaw was found in containers using nmstate/kubernetes-nmstate-handler. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.
Clone Of:
Environment:
Last Closed: 2021-10-28 02:03:18 UTC

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

Joshua Padman 2020-02-17 02:42:03 UTC — Description

It has been found that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the nmstate/kubernetes-nmstate-handler container.

Original bug:
~~https://bugzilla.redhat.com/show_bug.cgi?id=1791534~~

Joshua Padman 2020-02-17 02:42:07 UTC — Comment 1

Acknowledgments:

Name: Joseph LaMagna-Reiter (SPR Inc.)

Joshua Padman 2020-02-17 02:42:09 UTC — Comment 2

Statement:

By default this vulnerability is not exploitable in un-privilieged containers running on OpenShift Container Platform. This is because the system call SETUID and SETGID is blocked by the default seccomp policy.

~~Mark Cooper~~ 2021-10-28 02:03:18 UTC — Comment 11

Used fixcvenames on https://errata.devel.redhat.com/advisory/48747 and fixed the affects

Closing the old flaw bug

Note
You need to log in before you can comment on or make changes to this bug.