Bug 2121445 (CVE-2022-2989) - CVE-2022-2989 podman: possible information disclosure and modification

Keywords:	Security ×
Status:	NEW
Alias:	CVE-2022-2989
Product:	Security Response
Component:	vulnerability
Version:	unspecified
Hardware:	All
OS:	Linux
Priority:	low
Severity:	low
Target Milestone:	---
Assignee:	Red Hat Product Security
QA Contact:	
Docs Contact:	
URL:	
Whiteboard:	
Depends On:	🔒 2121540 🔒 2121541 🔒 2121542 🔒 2121533 🔒 2121538 🔒 2121539 🔒 2126485 🔒 2136268
Blocks:	🔒 2121446 🔒 2121448
TreeView+	depends on / blocked

Reported:	2022-08-25 13:30 UTC by Marian Rehak
Modified:	2022-11-15 15:59 UTC (History)
CC List:	14 users (show)
Fixed In Version:	
Doc Type:	If docs needed, set a value
Doc Text:	An incorrect handling of the supplementary groups in the Podman container engine might lead to the sensitive information disclosure or possible data modification if an attacker has direct access to the affected container where supplementary groups are used to set access permissions and is able to execute a binary code in that container.
Clone Of:	
Environment:	
Last Closed:	

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-2022:7822	0	None	None	None	2022-11-08 11:30:44 UTC
Red Hat Product Errata	RHSA-2022:8008	0	None	None	None	2022-11-15 09:57:41 UTC
Red	RHSA-	0	None	None	None	2022-

Hat Product Errata	2022:8431					11-15 15:59:18 UTC

Marian Rehak 2022-08-25 13:30:08 UTC Description

An incorrect handling of the supplementary groups in the Podman container engine might lead to the sensitive information disclosure or possible data modification if an attacker has direct access to the affected container where supplementary groups are used to set access permissions and is able to execute a binary code in that container.

Reference:

https://www.benthamsgaze.org/2022/08/22/vulnerability-in-linux-containers-investigation-and-mitigation/

John Helmert III 2022-09-19 20:06:38 UTC Comment 3

Looks like the patch is:
https://github.com/containers/podman/commit/5c7f28336171f0a5137edd274e45608120d31289

Seems unreleased.

Jindrich Novy 2022-09-20 08:30:50 UTC Comment 4

John, it's been replaced with
https://github.com/containers/podman/pull/15696 -
🔒 https://bugzilla.redhat.com/show_bug.cgi?id=2121542#c4

errata-xmlrpc 2022-11-08 11:30:42 UTC Comment 5

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2022:7822 https://access.redhat.com/errata/RHSA-2022:7822

errata-xmlrpc 2022-11-15 09:57:39 UTC Comment 6

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2022:8008 https://access.redhat.com/errata/RHSA-2022:8008

errata-xmlrpc 2022-11-15 15:59:16 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2022:8431 https://access.redhat.com/errata/RHSA-2022:8431

Note

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