Bug 2121453 (CVE-2022-2990) - CVE-2022-2990 buildah: possible information disclosure and modification

Keywords: Security ×

Status: NEW

Alias: CVE-2022-2990

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: 2126233 2121529 2121530 2121531 2121532 2121533 2125646 2136297

Blocks: 2121454 2121455

TreeView+ depends on / blocked

Reported: 2022-08-25 13:58 UTC by Marian Rehak

Modified: 2022-11-15 15:59 UTC (History)

CC List: 11 users (show)

Fixed In Version:

Doc Type: If docs needed, set a value

Doc Text: An incorrect handling of the supplementary groups in the Buildah 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
Github	containers buildah pull 4200	0	None	Merged	run: add container `gid` to additional groups	2022-08-29 07:28:10 UTC
Red Hat Product Errata	RHSA-2022:7457	0	None	None	None	2022-11-08 09:12:12 UTC

Red Hat Product Errata	RHSA-2022:7822	0	None	None	None	2022-11-08 11:30:47 UTC
Red Hat Product Errata	RHSA-2022:8008	0	None	None	None	2022-11-15 09:57:44 UTC
Red Hat Product Errata	RHSA-2022:8431	0	None	None	None	2022-11-15 15:59:19 UTC

Marian Rehak 2022-08-25 13:58:09 UTC Description

```
An incorrect handling of the supplementary groups in the
Buildah 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/
```

Przemyslaw Roguski 2022-08-25 18:34:38 UTC Comment 3

```
Upstream patch:
https://github.com/containers/buildah/pull/4200
```

errata-xmlrpc 2022-11-08 09:12:10 UTC Comment 5

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

  Red Hat Enterprise Linux 8

Via RHSA-2022:7457 https://access.redhat.com/errata/RHSA-
2022:7457
```

errata-xmlrpc 2022-11-08 11:30:44 UTC Comment 6

```
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 09:57:42 UTC Comment 7

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 15:59:17 UTC Comment 8

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.