Bug 1817651 (CVE-2020-10696) - CVE-2020-10696 buildah: Crafted input tar file may lead to local file overwrite during image build process

Keywords: Security ×

Status: CLOSED ERRATA

Alias: CVE-2020-10696

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: ~~1817687~~ ~~1817688~~ ~~1817694~~ ~~1817692~~ ~~1817693~~ ~~1817694~~ 1817738 1817739 1817740 1817741 1817742 1817743 1817744 1817745 1817746 1817747 1817791 1817792 1818120 1818121 1818122 1818125 1818126 1818127 1819046 1819047 1819048 1819049 1819325 1819326 1819327 1819328 1819329 1819330 1819331 1819332 1819333 1819334 1819391 1819393 1819429 1819430 1819431 1819432 1819809 1819810 1819811 1819812

Blocks: 1814229

TreeView+ depends on / blocked

Reported: 2020-03-26 17:49 UTC by Marco Benatto

Modified: 2021-02-16 20:23 UTC (History)

CC List: 37 users (show)

Fixed In Version: buildah-1.14.5

Doc Type: If docs needed, set a value

Doc Text: A path traversal flaw was found in Buildah. This flaw allows an attacker to trick a user into building a malicious container image hosted on an HTTP(s) server and then write files to the user's system anywhere that the user has permissions.

Clone Of:

Environment:

Last Closed: 2020-04-14 16:31:48 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	RHBA-2020:2066	0	None	None	None	2020-05-12 01:00:30 UTC
Red Hat Product Errata	RHSA-2020:1396	0	None	None	None	2020-04-14 15:37:56 UTC
Red Hat Product Errata	RHSA-2020:1401	0	None	None	None	2020-04-14 12:29:42 UTC
Red Hat Product Errata	RHSA-2020:1449	0	None	None	None	2020-04-22 15:41:43 UTC
Red Hat Product Errata	RHSA-2020:1926	0	None	None	None	2020-04-28 20:53:58 UTC
Red Hat Product Errata	RHSA-2020:1931	0	None	None	None	2020-04-28 20:54:33 UTC
Red Hat Product Errata	RHSA-2020:1932	0	None	None	None	2020-04-28 20:54:43 UTC
Red Hat Product Errata	RHSA-2020:2116	0	None	None	None	2020-05-12 19:50:39 UTC
Red Hat Product Errata	RHSA-2020:2117	0	None	None	None	2020-05-12 19:50:55 UTC

Marco Benatto 2020-03-26 17:49:45 UTC — Description

During buildah image building process a crafted tar file containing symlinks may lead buildah to overwrite any file which the running uid have write permissions, compromising confidentiality, integrity and possibly allowing code execution.

Marco Benatto 2020-03-26 17:50:58 UTC — Comment 1

Acknowledgments:

Name: Erik Sjölund

Marco Benatto 2020-03-26 17:52:36 UTC — Comment 3

Upstream commit for this issue:
https://github.com/containers/buildah/commit/c61925b8936e93a5e900f91b653a846f7ea3a9ed

Marco Benatto 2020-03-26 18:48:15 UTC — Comment 4

Created buildah tracking bugs for this issue:

Affects: fedora-30 [~~bug 1817687~~]
Affects: fedora-31 [~~bug 1817688~~]

Affects: openstack-rdo [~~bug 1817693~~]

Created podman tracking bugs for this issue:

Affects: fedora-30 [~~bug 1817691~~]
Affects: fedora-31 [~~bug 1817692~~]
Affects: openstack-rdo [~~bug 1817694~~]

Jason Shepherd 2020-03-27 02:20:26 UTC Comment 11

For openshift-3.11 openshift/imagebuilder does not depend on buildah, or podman. Also it doesn't allow a user to host a Dockerfile over HTTP.

Daniel Walsh 2020-03-27 13:50:21 UTC Comment 13

Note, while there is a fix for buildah, it has not been vendored into Podman yet.

We have a lot of other distributions using podman, we have to make sure they are in on this.

Marco Benatto 2020-04-03 13:32:34 UTC Comment 39

There's a issue on buildah during container image building process. Currently if buildah fails to fetch the content used as parameter for building, it tries to refetch it again without properly cleanup the build directory. An attack may leverage this by crafting a malicious input which will force buildah to overwrite any existing file which task's owner has write access.

Daniel Walsh 2020-04-06 13:55:49 UTC Comment 42

I agree this is low, no one is using podman on a Openshift nodes, directly, it is only being used for the install and maintenance of images.

Therefore noone is going to execute podman build.

errata-xmlrpc 2020-04-14 12:29:39 UTC Comment 43

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.2

Via RHSA-2020:1401 https://access.redhat.com/errata/RHSA-2020:1401

errata-xmlrpc 2020-04-14 15:37:54 UTC Comment 44

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.3

Via RHSA-2020:1396 https://access.redhat.com/errata/RHSA-2020:1396

Product Security DevOps Team 2020-04-14 16:31:48 UTC Comment 45

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-2020-10696

errata-xmlrpc 2020-04-22 15:41:41 UTC Comment 46

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.1

Via RHSA-2020:1449 https://access.redhat.com/errata/RHSA-2020:1449

Jason Shepherd 2020-04-24 01:27:28 UTC Comment 47

Statement:

While OpenShift Container Platform does include the vulnerable buildah code, it doesn't make use of the vulnerable function. Podman is also included in OpenShift Container Platform, but it isn't used to perform a build, so it has been given a low impact rating.

OpenShift Container Platform 3.11 now used podman from the RHEL Extra repository, and not the podman package shipped in the OpenShift 3.11 RPM repository. This issue is fixed in podman in RHEL Extras so we won't fix the podman package shipped in the OpenShift 3.11 RPM repository.

errata-xmlrpc 2020-04-28 20:53:56 UTC Comment 48

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2020:1926 https://access.redhat.com/errata/RHSA-2020:1926

errata-xmlrpc 2020-04-28 20:54:31 UTC Comment 49

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2020:1931 https://access.redhat.com/errata/RHSA-2020:1931

errata-xmlrpc 2020-04-28 20:54:41 UTC Comment 50

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2020:1932 https://access.redhat.com/errata/RHSA-2020:1932

errata-xmlrpc 2020-05-12 19:50:37 UTC Comment 51

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extras

Via RHSA-2020:2116 https://access.redhat.com/errata/RHSA-2020:2116

errata-xmlrpc 2020-05-12 19:50:53 UTC Comment 52

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7 Extras

Via RHSA-2020:2117 https://access.redhat.com/errata/RHSA-2020:2117