Subscriptions | Downloads | Red Hat Console | Get Support

Re
Cu

ed Hat Log In

We use cookies on this site

Click "Agree and proceed with standard settings" to accept all cookies, including functional and advertising cookies, and go directly to the site. Or click "Proceed with Required Cookies only" to continue directly to the site with only Required Cookies. You can also click "View cookies preferences" for a detailed description of the types of cookies we use and to customize your cookie selection.

Agree and proceed with standard settings

Proceed with Required Cookies only

View cookie preferences

Privacy Statement

CVE-20

Public on 14 o

Last Modified

IMPORTANT

Description

A flaw was found in the way sudo implemented running commands with arbitrary user ID. If a sudoers entry is written to allow the attacker to run a command as any user except root, this flaw can be used by the attacker to bypass that restriction.

Statement

This flaw only affects specific, non-default configurations of sudo, in which sudoers configuration entry allows a user to run a command as any user except root, for example:

someuser myhost = (ALL, !root) /usr/bin/somecommand

This configuration allows user "someuser" to run somecommand as any other user except root. However, this flaw also allows someuser to run somecommand as root by specifying the target user using the numeric id of -1. Only the specified command can be run, this flaw does NOT allow user to run other commands that those specified in the sudoers configuration.

Any other configurations of sudo (including configurations that allow user to run commands as any user including root and configurations that allow user to run command as a specific other user) are NOT affected by this flaw.

Red Hat Virtualization Hypervisor includes an affected version of sudo, however the default configuration is not vulnerable to this flaw.

Mitigation

This vulnerability only affects configurations of sudo that have a runas user list that includes an exclusion of root. The most simple example is:

External references

- https://www.cve.org/CVERecord?id=CVE-2019-14287
- https://nvd.nist.gov/vuln/detail/CVE-2019-14287
- https://www.sudo.ws/alerts/minus_1_uid.html

```
someuser ALL=(ALL, !root) /usr/bin/somecommand
```

The exclusion is specified using an excalamation mark (!). In this example, the "root" user is specified by name. The root user may also be identified in other ways, such as by user id:

```
someuser ALL=(ALL, !#0) /usr/bin/somecommand
```

or by reference to a runas alias:

```
Runas_Alias MYGROUP = root, adminuser
someuser ALL=(ALL, !MYGROUP) /usr/bin/somecommand
```

To ensure your sudoers configuration is not affected by this vulnerability, we recommend examining each sudoers entry that includes the `!` character in the runas specification, to ensure that the root user is not among the exclusions. These can be found in the /etc/sudoers file or files under /etc/sudoers.d.

Additional information

- Bugzilla 1760531: sudo: Privilege escalation via 'Runas' specification with 'ALL' keyword
- CWE-267: Privilege Defined With Unsafe Actions
- FAQ: Frequently asked questions about CVE-2019-14287

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata | Clear all

Products / Services	**Components**	**State**	**Errata**	**Release Date**
Red Hat Enterprise Linux 5 Extended Lifecycle Support	sudo	Fixed	RHSA-2019:4191	10 décembre 2019
Red Hat Enterprise Linux 6	sudo	Fixed	RHSA-2019:3755	6 novembre 2019
Red Hat Enterprise Linux 6.5 Advanced Update Support	sudo	Fixed	RHSA-2019:3895	18 novembre 2019
Red Hat Enterprise Linux 6.6 Advanced Update Support	sudo	Fixed	RHSA-2019:3754	6 novembre 2019
Red Hat Enterprise Linux 7	sudo	Fixed	RHSA-2019:3197	24 octobre 2019

Red Hat Enterprise Linux 7.2 Advanced Update Support	sudo	Fixed	RHSA-2019:3278	31 octobre 2019
Red Hat Enterprise Linux 7.2 Telco Extended Update Support	sudo	Fixed	RHSA-2019:3278	31 octobre 2019
Red Hat Enterprise Linux 7.2 Update Services for SAP Solutions	sudo	Fixed	RHSA-2019:3278	31 octobre 2019
Red Hat Enterprise Linux 7.3 Advanced Update Support	sudo	Fixed	RHSA-2019:3219	29 octobre 2019
Red Hat Enterprise Linux 7.3 Telco Extended Update Support	sudo	Fixed	RHSA-2019:3219	29 octobre 2019

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

1-10 of 22 « ‹ 1 of 3 › »

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	7	8.8
Attack Vector	Local	Network
Attack Complexity	High	Low
Privileges Required	Low	Low
User Interaction	None	None
Scope	Unchanged	Unchanged

CVSS v3 Vector

Red Hat: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Confidentiality Impact	High	High
Integrity Impact	High	High
Availability Impact	High	High

Acknowledgements

Red Hat would like to thank the Sudo project for reporting this issue. Upstream acknowledges Joe Vennix (Apple Information Security) as the original reporter.

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors? >
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability? >
- What can I do if my product is listed as "Will not fix"? >
- What can I do if my product is listed as "Fix deferred"? >
- What is a mitigation? >
- I have a Red Hat product but it is not in the above list, is it affected? >
- Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected? >

Not sure what something means? Check out our Security Glossary.

This page is generated automatically and has not been checked for errors or omissions.
For clarification or corrections please contact Red Hat Product Security.

Last Modified: 13 septembre 2024 à 03:57:31 UTC

Red Hat

Quick Links	Help	Site Info	Related Sites
Downloads	Contact Us	Trust Red Hat	redhat.com

Subscriptions

Support Cases

Customer Service

Product Documentation

Customer Portal FAQ

Log-in Assistance

Browser Support Policy

Accessibility

Awards and Recognition

Colophon

developers.redhat.com

connect.redhat.com

cloud.redhat.com

✓ All systems operational

About Red Hat Jobs Events Locations Contact Red Hat Red Hat Blog Diversity, equity, and inclusion Cool Stuff Store Red Hat Summit

Privacy statement Terms of use All policies and guidelines Digital accessibility Cookie preferences