



# CVE-2024-10963

Public on November 7, 2024

Last Modified: November 10, 2024 at 1:50:32 PM UTC

IMPORTANT

## Important Impact

What does this mean?

7.4

[CVSS v3 Score Breakdown](#)

## Description

The CVE Program describes this issue as:

A vulnerability was found in pam\_access due to the improper handling of tokens in access.conf, interpreted as hostnames. This flaw allows attackers to bypass access restrictions by spoofing hostnames, undermining configurations designed to limit access to specific TTYs or services. The flaw poses a risk in environments relying on these configurations for local access control.

## Mitigation

To reduce the risk, administrators should ensure that no DNS hostname matches local TTY or service names used in pam\_access. Additionally, implement DNSSEC to prevent spoofing of DNS responses. For stronger protection, consider reconfiguring pam\_access to only accept fully qualified domain names (FQDNs) in access.conf

## Additional information

- Bugzilla 2324291: pam: Improper Hostname Interpretation in pam\_access Leads to Access Control Bypass
- CWE-287: Improper Authentication

- [FAQ: Frequently asked questions about CVE-2024-10963](#)

### External references

- <https://www.cve.org/CVERecord?id=CVE-2024-10963>
- <https://nvd.nist.gov/vuln/detail/CVE-2024-10963>

## Affected Packages and Issued Red Hat Security Errata

Search:

Filter by:

Products / Services

Components

State

Errata

[Clear all](#)

Products / Services	Components	State	Errata	Released Date
Red Hat Enterprise Linux 7	pam	Out of support scope		
Red Hat Enterprise Linux 8	pam	Affected		

Red Hat Enterprise Linux 9	pam	Affected
Red Hat OpenShift Container Platform 4	rhcos	Affected

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 4

<<<>>>

1 of 1

## 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).

The following CVSS metrics and score provided are preliminary and subject to review.

### CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	7.4	N/A
Attack Vector	Network	N/A
Attack Complexity	High	N/A
Privileges Required	None	N/A
User Interaction	None	N/A

	Red Hat	NVD
Scope	Unchanged	N/A
Confidentiality Impact	High	N/A
Integrity Impact	High	N/A
Availability Impact	None	N/A

### CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

### 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: November 10, 2024 at 1:50:32 PM UTC  
CVE description copyright © 2021, [The MITRE Corporation](#)



---

Quick Links

---

Help


---

Site Info

---

Related Sites

---

 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

---

© 2024 Red Hat, Inc.

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)