CVE

VEX
Public o
Last mo

Jump to section

Description

A flaw was found in Samba. The smbd service daemon does not pick up group membership changes when re-authenticating an expired SMB session. This issue can expose file shares until clients disconnect and then connect again.

Additional information

- Bugzilla 2370453: samba: smbd doesn't pick up group membership changes when re-authenticating an expired SMB session
- CWE-552: Files or Directories Accessible to External Parties

External references

- https://www.cve.org/CVERecord?id=CVE-2025-0620
- https://nvd.nist.gov/vuln/detail/CVE-2025-0620
- https://www.samba.org/samba/security/CVE-2025-0620.html

Affected Packages and Issued Red Hat Security Errata

Search:

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

Products / Services	Red Hat Enterprise Linux 10
Components	samba
State	Fix deferred
Justification	None
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 6
Components	samba
State	Not affected

Justification	Vulnerable Code not Present
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 6

1-10 of 7

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.

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	4.9	4.9
Attack Vector	Network	Network

	Red Hat	NVD
Attack Complexity	Low	Low
Privileges Required	High	High
User Interaction	None	None
Scope	Unchanged	Unchanged
Confidentiality Impact	High	High
Integrity Impact	None	None
Availability Impact	None	None

CVSS v3 Vector

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

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

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: January 8, 2026 at 3:03:51 AM UTC

Partial system outage