



# CVE-2023-3961

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-3961
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-03 13:15:00 UTC
<b>Updated</b>	2024-01-02 21:15:00 UTC
<b>Description</b>	A path traversal vulnerability was identified in Samba when processing client pipe names connecting to Unix domain socket

## Risk And Classification

**Problem Types:** CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	39	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Storage</a>	3.0	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	All	All	All	All

## References

Reference	Source
2241881 – (CVE-2023-3961) CVE-2023-3961 samba: smbd allows client access to unix domain sockets on the file system as root	MISC
RHSA-2023:7464	
security.netapp.com/advisory/ntap-20231124-0002	
15422 – (CVE-2023-3961) CVE-2023-3961 [SECURITY] Unsanitized client pipe name passed to local_np_connect()	MISC
RHSA-2023:7371	
Samba - Security Announcement Archive	MISC
[SECURITY] Fedora 39 Update: samba-4.19.2-1.fc39 - package-announce - Fedora Mailing-Lists	MISC
Red Hat	MISC
Red Hat	

RHSA-2023:7408	
RHSA-2023:7467	
cve-details	MISC
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">161070</a> Oracle Enterprise Linux Security Update for samba (ELSA-2023-6744)
<a href="#">161196</a> Oracle Enterprise Linux Security Update for samba (ELSA-2023-7467)
<a href="#">242260</a> Red Hat Update for samba (RHSA-2023:6209)
<a href="#">242318</a> Red Hat Update for samba (RHSA-2023:6744)
<a href="#">242484</a> Red Hat Update for samba (RHSA-2023:7408)
<a href="#">242507</a> Red Hat Update for samba (RHSA-2023:7467)
<a href="#">242508</a> Red Hat Update for samba (RHSA-2023:7464)
<a href="#">284612</a> Fedora Security Update for samba (FEDORA-2023-7eb8cbf1a5)
<a href="#">284682</a> Fedora Security Update for samba (FEDORA-2023-fff0c857d6)
<a href="#">285191</a> Fedora Security Update for samba (FEDORA-2023-8c9251e479)
<a href="#">356630</a> Amazon Linux Security Advisory for samba : ALAS2023-2023-416
<a href="#">503395</a> Alpine Linux Security Update for samba
<a href="#">505937</a> Alpine Linux Security Update for samba
<a href="#">6000310</a> Debian Security Update for samba (DSA 5525-1)
<a href="#">710873</a> Gentoo Linux Samba Multiple Vulnerabilities (GLSA 202402-28)
<a href="#">755069</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:4046-1)
<a href="#">941395</a> AlmaLinux Security Update for samba (ALSA-2023:6744)
<a href="#">941422</a> AlmaLinux Security Update for samba (ALSA-2023:7467)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**