



# CVE-2023-42669

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

## Summary

<b>CVE</b>	CVE-2023-42669
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-06 07:15:00 UTC
<b>Updated</b>	2023-11-14 18:20:00 UTC
<b>Description</b>	A vulnerability was found in Samba's "rpcecho" development server, a non-Windows RPC server used to test Samba's DCE

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	9.0_s390x	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems Eus</a>	9.0_s390x	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	9.0_ppc64le	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	9.0_ppc64le	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	S
<a href="#">cve-details</a>	M
<a href="#">2241884 - (CVE-2023-42669) CVE-2023-42669 samba: "rpcecho" development server allows denial of service via sleep() call on AD DC</a>	M
<a href="#">Red Hat</a>	M
<a href="#">Red Hat</a>	
<a href="#">Samba - Security Announcement Archive</a>	M

15474 – (CVE-2023-42669) [SECURITY] CVE-2023-42669 rpcecho, enabled and running in AD DC, allows blocking sleep on request	M
CVE Program record	C
NVD vulnerability detail	N

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="#">199820</a> Ubuntu Security Notification for Samba Vulnerabilities (USN-6425-1)
<a href="#">199907</a> Ubuntu Security Notification for Samba Vulnerabilities (USN-6425-3)
<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="#">242602</a> Red Hat Update for samba (RHSA-2023:7371)
<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="#">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="#">673574</a> EulerOS Security Update for samba (EulerOS-SA-2023-3286)
<a href="#">673680</a> EulerOS Security Update for samba (EulerOS-SA-2023-3258)
<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="#">755081</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:4059-1)
<a href="#">755106</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:4096-1)
<a href="#">941395</a> AlmaLinux Security Update for samba (ALSA-2023:6744)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)