



# CVE-2022-0336

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-0336
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-29 15:15:00 UTC
<b>Updated</b>	2023-09-17 09:15:00 UTC
<b>Description</b>	The Samba AD DC includes checks when adding service principals names (SPNs) to an account to ensure that SPNs do not

## Risk And Classification

**Problem Types:** CWE-276

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	All	All	All	All

## References

### Reference

- [Red Hat Customer Portal - Access to 24x7 support and knowledge](#)
- [Samba: Multiple Vulnerabilities \(GLSA 202309-06\) — Gentoo security](#)
- [14950 – \(CVE-2022-0336\) CVE-2022-0336 \[SECURITY\] Re-adding an SPN skips subsequent SPN conflict checks](#)
- [CVE-2022-0336: s4/dsdb/samldb: Don't return early when an SPN is re-a... · samba-team/samba@1a5dc81 · GitHub](#)
- [CVE-2022-0336: pytest: Add a test for an SPN conflict with a re-added... · samba-team/samba@c58ede4 · GitHub](#)
- [Samba - Security Announcement Archive](#)
- [2046134 – \(CVE-2022-0336\) CVE-2022-0336 samba: Samba AD users with permission to write to an account can impersonate arbitrary servi](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

179066	Debian Security Update for samba (DSA 5071-1)
179080	Debian Security Update for samba (CVE-2022-0336)
198651	Ubuntu Security Notification for Samba Vulnerabilities (USN-5260-1)
282312	Fedora Security Update for samba (FEDORA-2022-50da406d40)
282317	Fedora Security Update for samba (FEDORA-2022-055efdd9dc)
296057	Oracle Solaris 11.4 Support Repository Update (SRU) 44.113.4 Missing (bulletinapr2022)
354310	Amazon Linux Security Advisory for samba : ALAS2022-2022-022
354496	Amazon Linux Security Advisory for samba : ALAS2022-2022-224
354550	Amazon Linux Security Advisory for samba : ALAS-2022-224
355336	Amazon Linux Security Advisory for samba : ALAS2023-2023-032
502620	Alpine Linux Security Update for samba
503810	Alpine Linux Security Update for samba
671442	EulerOS Security Update for samba (EulerOS-SA-2022-1459)
671468	EulerOS Security Update for samba (EulerOS-SA-2022-1438)
671569	EulerOS Security Update for samba (EulerOS-SA-2022-1586)
671623	EulerOS Security Update for samba (EulerOS-SA-2022-1666)
671635	EulerOS Security Update for samba (EulerOS-SA-2022-1652)
690784	Free Berkeley Software Distribution (FreeBSD) Security Update for samba (8579074c-839f-11ec-a3b2-005056a311d1)
710751	Gentoo Linux Samba Multiple Vulnerabilities (GLSA 202309-06)
751680	OpenSUSE Security Update for samba (openSUSE-SU-2022:0283-1)
751683	SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0323-1)
751994	SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0283-1)
903851	Common Base Linux Mariner (CBL-Mariner) Security Update for samba (10741)

© 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](#)**