



CVE-2023-4154

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-4154
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-07 20:15:00 UTC
Updated	2023-11-15 15:40:00 UTC
Description	A design flaw was found in Samba's DirSync control implementation, which exposes passwords and secrets in Active Direc

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	All	All	All	All

References

Reference

- 2241883 – (CVE-2023-4154) CVE-2023-4154 samba: AD DC password exposure to privileged users and RODCs
- 15424 – (CVE-2023-4154) CVE-2023-4154 [SECURITY] dirsnc allows SYSTEM access with only "GUID_DRS_GET_CHANGES" right, not "cve-details"
- Samba - Security Announcement Archive
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

199820 Ubuntu Security Notification for Samba Vulnerabilities (USN-6425-1)

199907 Ubuntu Security Notification for Samba Vulnerabilities (USN-6425-3)

2014105 Ubuntu Security Notification for Samba Vulnerabilities (USN-6425-5)

284612 Fedora Security Update for samba (FEDORA-2023-7eb8cb11a5)
284682 Fedora Security Update for samba (FEDORA-2023-fff0c857d6)
285191 Fedora Security Update for samba (FEDORA-2023-8c9251e479)
503395 Alpine Linux Security Update for samba
505937 Alpine Linux Security Update for samba
6000310 Debian Security Update for samba (DSA 5525-1)
673574 EulerOS Security Update for samba (EulerOS-SA-2023-3286)
673680 EulerOS Security Update for samba (EulerOS-SA-2023-3258)
710873 Gentoo Linux Samba Multiple Vulnerabilities (GLSA 202402-28)
755069 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:4046-1)
755081 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:4059-1)
755106 SUSE Enterprise Linux Security Update for samba (SUSE-SU-2023:4096-1)

© [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](#)