



CVE-2020-25721

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-25721 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-03-16 15:15:00 UTC |
| Updated | 2023-09-17 09:15:00 UTC |
| Description | Kerberos acceptors need easy access to stable AD identifiers (eg objectSid). Samba as an AD DC now provides a way for |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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

References

| Reference | Source |
|---|--------|
| Samba - Security Announcement Archive | MISC |
| Samba: Multiple Vulnerabilities (GLSA 202309-06) — Gentoo security | GENT |
| 2021728 – (CVE-2020-25721) CVE-2020-25721 samba: Kerberos acceptors need easy access to stableAD identifiers (eg objectSid) | MISC |
| 14725 – [SECURITY] Andrew's Kerberos Concerns (November 9 2021) | MISC |
| CVE Program record | CVE.C |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178884](#) Debian Security Update for samba (DSA 5003-1)

[198583](#) Ubuntu Security Notification for Samba Vulnerability (USN-5142-1)

[202309-06](#) Gentoo Security Advisory for Samba (GLSA 202309-06)

| |
|---|
| 282091 Fedora Security Update for treeipa (FEDORA-2021-1d7704/c61) |
| 282156 Fedora Security Update for freeipa (FEDORA-2021-12af2614da) |
| 296061 Oracle Solaris 11.4 Support Repository Update (SRU) 42.113.1 Missing (CPUJAN2022) |
| 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 |
| 501490 Alpine Linux Security Update for samba |
| 501779 Alpine Linux Security Update for samba |
| 502027 Alpine Linux Security Update for samba |
| 504394 Alpine Linux Security Update for samba |
| 671280 EulerOS Security Update for samba (EulerOS-SA-2022-1246) |
| 671315 EulerOS Security Update for samba (EulerOS-SA-2022-1258) |
| 671372 EulerOS Security Update for samba (EulerOS-SA-2022-1295) |
| 671384 EulerOS Security Update for samba (EulerOS-SA-2022-1311) |
| 690244 Free Berkeley Software Distribution (FreeBSD) Security Update for samba (646923b0-41c7-11ec-a3b2-005056a311d1) |
| 710751 Gentoo Linux Samba Multiple Vulnerabilities (GLSA 202309-06) |
| 751345 OpenSUSE Security Update for samba and ldb (openSUSE-SU-2021:3647-1) |

© [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](#)