



# CVE-2020-27840

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

## Summary

<b>CVE</b>	CVE-2020-27840
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-12 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	A flaw was found in samba. Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	All	All	All	All

## References

Reference	Source	Link	Tag
[SECURITY] Fedora 33 Update: libldb-2.2.1-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
1941400 – (CVE-2020-27840) CVE-2020-27840 samba: Heap corruption via crafted DN strings	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
[SECURITY] Fedora 32 Update: samba-4.12.14-0.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 2611-1] ldb security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
[SECURITY] Fedora 33 Update: libldb-2.2.1-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Debian -- Security Information -- DSA-4884-1 ldb	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
March 2021 Samba Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
Samba: Multiple vulnerabilities (GLSA 202105-22) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	

[SECURITY] Fedora 34 Update: samba-4.14.2-0.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 32 Update: samba-4.12.14-0.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 34 Update: samba-4.14.2-0.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
Samba - Security Announcement Archive	MISC	<a href="https://www.samba.org">www.samba.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	car

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">174841</a> SUSE Enterprise Linux Security update for ldb (SUSE-SU-2021:0945-1)
<a href="#">174843</a> SUSE Enterprise Linux Security update for ldb (SUSE-SU-2021:0944-1)
<a href="#">174860</a> SUSE Enterprise Linux Security Update for ldb (SUSE-SU-2021:0945-1)
<a href="#">174862</a> SUSE Enterprise Linux Security update for ldb (SUSE-SU-2021:0944-1)
<a href="#">174966</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2021:1444-1)
<a href="#">174982</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2021:1498-1)
<a href="#">178491</a> Debian Security Update for ldb (DSA 4884-1)
<a href="#">178508</a> Debian Security Update for ldb (DLA 2611-1)
<a href="#">198308</a> Ubuntu Security Notification for Ldb Vulnerabilities (USN-4888-1)
<a href="#">281411</a> Fedora Security Update for libldb (FEDORA-2021-1a8e93a285)
<a href="#">281412</a> Fedora Security Update for libldb (FEDORA-2021-c93a3a5d3f)
<a href="#">281423</a> Fedora Security Update for libldb (FEDORA-2021-c2d8628d33)
<a href="#">500625</a> Alpine Linux Security Update for samba
<a href="#">501491</a> Alpine Linux Security Update for samba
<a href="#">501780</a> Alpine Linux Security Update for samba
<a href="#">504391</a> Alpine Linux Security Update for samba
<a href="#">670411</a> EulerOS Security Update for samba (EulerOS-SA-2021-1988)
<a href="#">670415</a> EulerOS Security Update for libldb (EulerOS-SA-2021-1984)
<a href="#">670434</a> EulerOS Security Update for samba (EulerOS-SA-2021-2066)
<a href="#">670445</a> EulerOS Security Update for samba (EulerOS-SA-2021-2055)

<a href="#">670468</a> EulerOS Security Update for samba (EulerOS-SA-2021-2229)
<a href="#">670469</a> EulerOS Security Update for libldb (EulerOS-SA-2021-2222)
<a href="#">670639</a> EulerOS Security Update for libldb (EulerOS-SA-2021-2397)
<a href="#">670688</a> EulerOS Security Update for samba (EulerOS-SA-2021-2446)
<a href="#">670863</a> EulerOS Security Update for libldb (EulerOS-SA-2021-2591)
<a href="#">670896</a> EulerOS Security Update for libldb (EulerOS-SA-2021-1984)
<a href="#">670994</a> EulerOS Security Update for samba (EulerOS-SA-2021-2615)
<a href="#">690216</a> Free Berkeley Software Distribution (FreeBSD) Security Update for samba (1f6d97da-8f72-11eb-b3f1-005056a311d1)
<a href="#">710094</a> Gentoo Linux Samba Multiple vulnerabilities (GLSA 202105-22)
<a href="#">750236</a> OpenSUSE Security Update for samba (openSUSE-SU-2021:0636-1)
<a href="#">750299</a> OpenSUSE Security Update for ldb (openSUSE-SU-2021:0469-1)
<a href="#">751157</a> OpenSUSE Security Update for samba (openSUSE-SU-2021:3187-1)
<a href="#">751680</a> OpenSUSE Security Update for samba (openSUSE-SU-2022:0283-1)
<a href="#">751994</a> SUSE Enterprise Linux Security Update for samba (SUSE-SU-2022:0283-1)
<a href="#">901618</a> Common Base Linux Mariner (CBL-Mariner) Security Update for samba (7351)

© [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](#)**