



# CVE-2020-10700

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

## Summary

<b>CVE</b>	CVE-2020-10700
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-05-04 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:14:00 UTC
<b>Description</b>	A use-after-free flaw was found in the way samba AD DC LDAP servers, handled 'Paged Results' control is combined with t

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	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>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	All	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	All	All	All	All

## References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:1023-1: important: Security update	SUSE	<a href="#">lists.opensus</a>
[SECURITY] Fedora 32 Update: samba-4.12.2-0.fc32.1 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedorapr</a>
1825731 – (CVE-2020-10700) CVE-2020-10700 samba: Use-after-free in Samba AD DC LDAP Server with ASQ	CONFIRM	<a href="#">bugzilla.redh</a>
[SECURITY] Fedora 32 Update: samba-4.12.2-0.fc32.1 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedorapr</a>

[security-announce] openSUSE-SU-2020:1313-1: important: Security update	SUSE	<a href="https://lists.opensuse.org/">lists.opensuse.org</a>
Samba: Multiple vulnerabilities (GLSA 202007-15) — Gentoo security	GENTOO	<a href="https://security.gentoo.org/">security.gentoo.org</a>
Samba - Security Announcement Archive	MISC	<a href="https://www.samba.org/">www.samba.org</a>
[SECURITY] Fedora 31 Update: libldb-2.0.10-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: samba-4.10.15-0.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: libldb-2.0.10-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: samba-4.10.15-0.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[500627](#) Alpine Linux Security Update for samba

[504387](#) Alpine Linux Security Update for samba

© [CVE.report](https://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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org/). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)