

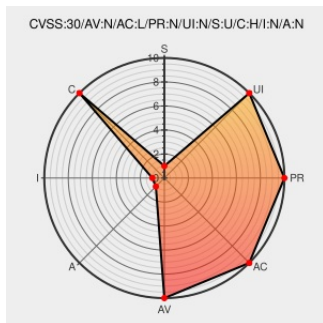


CVE-2015-5330

Published on: 12/29/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

CVE-2015-5330

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Samba](#) from [Samba](#) contain the following vulnerability:

ldb before 1.1.24, as used in the AD LDAP server in Samba 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, mishandles string lengths, which allows remote attackers to obtain sensitive information from daemon heap memory by sending crafted packets and then reading (1) an error message or (2) a database value.

CVE-2015-5330 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
USN-2855-1: Samba vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2855-1
[security-announce] SUSE-SU-	lists.opensuse.org	SUSE SUSE-SU-2015-2304

[security-announce] SUSE-SU-2015:2304-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:2304
git.samba.org - samba.git/commit	git.samba.org text/xml	 CONFIRM git.samba.org/?p=samba.git;a=commit;h=a118d4220ed85749c07fb43c1229d9e2fecbea6b
Samba: Multiple vulnerabilities (GLSA 201612-47) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201612-47
git.samba.org - samba.git/commit	git.samba.org text/xml	 CONFIRM git.samba.org/?p=samba.git;a=commit;h=ba5dbda6d0174a59d221c45cca52ecd232820d48
Bug 1281326 – CVE-2015-5330 samba, libldb: remote memory read in the Samba LDAP server	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1281326
[security-announce] SUSE-SU-2016:0032-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:0032
git.samba.org - samba.git/commit	git.samba.org text/xml	 CONFIRM git.samba.org/?p=samba.git;a=commit;h=f36cb71c330a52106e36028b3029d952257baf15
[security-announce] openSUSE-SU-2016:1107-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:1107
Samba ldb CVE-2015-5330 Multiple Information Disclosure Vulnerabilities	cve.report (archive) text/html	 BID 79734
[security-announce] SUSE-SU-2016:0164-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:0164
Samba Multiple Flaws Let Remote Users Access Data and Files, Obtain Potentially Sensitive Information, and Deny Service - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1034493
git.samba.org - samba.git/commit	git.samba.org text/xml	 CONFIRM git.samba.org/?p=samba.git;a=commit;h=0454b95657846fcec0f51b6f1194faac02518bd
[security-announce] openSUSE-SU-2015:2354-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2354
Samba - Security Announcement Archive	Vendor Advisory www.samba.org text/html	 CONFIRM www.samba.org/samba/security/CVE-2015-5330.html
[security-announce] openSUSE-SU-2015:2356-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2356
git.samba.org - samba.git/commit	git.samba.org text/xml	 CONFIRM git.samba.org/?p=samba.git;a=commit;h=538d305de91e34a2938f5f219f18bf0e1918763f
[security-announce] openSUSE-SU-2016:1064-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:1064
Oracle Linux Bulletin - January 2016	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html

git.samba.org - samba.git/commit	git.samba.org text/xml	 CONFIRM git.samba.org/?p=samba.git;a=commit;h=7f51ec8c4ed9ba1f53d722e44fb6fb3cde933b72
Debian -- Security Information -- DSA-3433-1 samba	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3433
USN-2856-1: ldb vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2856-1
[security-announce] openSUSE-SU-2016:1106-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:1106
USN-2855-2: Samba regression Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2855-2
[security-announce] SUSE-SU-2015:2305-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:2305

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	4.0.0	All	All	All
Application	Samba	Samba	4.0.1	All	All	All
Application	Samba	Samba	4.0.10	All	All	All
Application	Samba	Samba	4.0.11	All	All	All
Application	Samba	Samba	4.0.12	All	All	All
Application	Samba	Samba	4.0.13	All	All	All
Application	Samba	Samba	4.0.14	All	All	All
Application	Samba	Samba	4.0.15	All	All	All
Application	Samba	Samba	4.0.16	All	All	All
Application	Samba	Samba	4.0.17	All	All	All
Application	Samba	Samba	4.0.18	All	All	All
Application	Samba	Samba	4.0.19	All	All	All
Application	Samba	Samba	4.0.2	All	All	All
Application	Samba	Samba	4.0.20	All	All	All
Application	Samba	Samba	4.0.21	All	All	All
Application	Samba	Samba	4.0.22	All	All	All
Application	Samba	Samba	4.0.23	All	All	All

Application	Samba	Samba	4.0.24	All	All	All
Application	Samba	Samba	4.0.3	All	All	All
Application	Samba	Samba	4.0.4	All	All	All
Application	Samba	Samba	4.0.5	All	All	All
Application	Samba	Samba	4.0.6	All	All	All
Application	Samba	Samba	4.0.7	All	All	All
Application	Samba	Samba	4.0.8	All	All	All
Application	Samba	Samba	4.0.9	All	All	All
Application	Samba	Samba	4.1.0	All	All	All
Application	Samba	Samba	4.1.1	All	All	All
Application	Samba	Samba	4.1.10	All	All	All
Application	Samba	Samba	4.1.11	All	All	All
Application	Samba	Samba	4.1.12	All	All	All
Application	Samba	Samba	4.1.13	All	All	All
Application	Samba	Samba	4.1.14	All	All	All
Application	Samba	Samba	4.1.15	All	All	All
Application	Samba	Samba	4.1.16	All	All	All
Application	Samba	Samba	4.1.17	All	All	All
Application	Samba	Samba	4.1.18	All	All	All
Application	Samba	Samba	4.1.19	All	All	All
Application	Samba	Samba	4.1.2	All	All	All
Application	Samba	Samba	4.1.20	All	All	All
Application	Samba	Samba	4.1.21	All	All	All
Application	Samba	Samba	4.1.3	All	All	All
Application	Samba	Samba	4.1.4	All	All	All
Application	Samba	Samba	4.1.5	All	All	All
Application	Samba	Samba	4.1.6	All	All	All
Application	Samba	Samba	4.1.7	All	All	All
Application	Samba	Samba	4.1.8	All	All	All
Application	Samba	Samba	4.1.9	All	All	All
Application	Samba	Samba	4.2.0	All	All	All
Application	Samba	Samba	4.2.1	All	All	All
Application	Samba	Samba	4.2.2	All	All	All
Application	Samba	Samba	4.2.3	All	All	All
Application	Samba	Samba	4.2.4	All	All	All

Application	Samba	Samba	4.2.5	All	All	All
Application	Samba	Samba	4.2.6	All	All	All
Application	Samba	Samba	4.3.0	All	All	All
Application	Samba	Samba	4.3.1	All	All	All
Application	Samba	Samba	4.3.2	All	All	All
Application	Samba	Samba	4.0.0	All	All	All
Application	Samba	Samba	4.0.1	All	All	All
Application	Samba	Samba	4.0.10	All	All	All
Application	Samba	Samba	4.0.11	All	All	All
Application	Samba	Samba	4.0.12	All	All	All
Application	Samba	Samba	4.0.13	All	All	All
Application	Samba	Samba	4.0.14	All	All	All
Application	Samba	Samba	4.0.15	All	All	All
Application	Samba	Samba	4.0.16	All	All	All
Application	Samba	Samba	4.0.17	All	All	All
Application	Samba	Samba	4.0.18	All	All	All
Application	Samba	Samba	4.0.19	All	All	All
Application	Samba	Samba	4.0.2	All	All	All
Application	Samba	Samba	4.0.20	All	All	All
Application	Samba	Samba	4.0.21	All	All	All
Application	Samba	Samba	4.0.22	All	All	All
Application	Samba	Samba	4.0.23	All	All	All
Application	Samba	Samba	4.0.24	All	All	All
Application	Samba	Samba	4.0.3	All	All	All
Application	Samba	Samba	4.0.4	All	All	All
Application	Samba	Samba	4.0.5	All	All	All
Application	Samba	Samba	4.0.6	All	All	All
Application	Samba	Samba	4.0.7	All	All	All
Application	Samba	Samba	4.0.8	All	All	All
Application	Samba	Samba	4.0.9	All	All	All
Application	Samba	Samba	4.1.0	All	All	All
Application	Samba	Samba	4.1.1	All	All	All
Application	Samba	Samba	4.1.10	All	All	All
Application	Samba	Samba	4.1.11	All	All	All
Application	Samba	Samba	4.1.12	All	All	All
Application	Samba	Samba	4.1.13	All	All	All

Application	Samba	Samba	4.1.13	All	All	All
Application	Samba	Samba	4.1.14	All	All	All
Application	Samba	Samba	4.1.15	All	All	All
Application	Samba	Samba	4.1.16	All	All	All
Application	Samba	Samba	4.1.17	All	All	All
Application	Samba	Samba	4.1.18	All	All	All
Application	Samba	Samba	4.1.19	All	All	All
Application	Samba	Samba	4.1.2	All	All	All
Application	Samba	Samba	4.1.20	All	All	All
Application	Samba	Samba	4.1.21	All	All	All
Application	Samba	Samba	4.1.3	All	All	All
Application	Samba	Samba	4.1.4	All	All	All
Application	Samba	Samba	4.1.5	All	All	All
Application	Samba	Samba	4.1.6	All	All	All
Application	Samba	Samba	4.1.7	All	All	All
Application	Samba	Samba	4.1.8	All	All	All
Application	Samba	Samba	4.1.9	All	All	All
Application	Samba	Samba	4.2.0	All	All	All
Application	Samba	Samba	4.2.1	All	All	All
Application	Samba	Samba	4.2.2	All	All	All
Application	Samba	Samba	4.2.3	All	All	All
Application	Samba	Samba	4.2.4	All	All	All
Application	Samba	Samba	4.2.5	All	All	All
Application	Samba	Samba	4.2.6	All	All	All
Application	Samba	Samba	4.3.0	All	All	All
Application	Samba	Samba	4.3.1	All	All	All
Application	Samba	Samba	4.3.2	All	All	All
cpe:2.3:a:samba:samba:4.0.0:*****:						
cpe:2.3:a:samba:samba:4.0.1:*****:						
cpe:2.3:a:samba:samba:4.0.10:*****:						
cpe:2.3:a:samba:samba:4.0.11:*****:						
cpe:2.3:a:samba:samba:4.0.12:*****:						
cpe:2.3:a:samba:samba:4.0.13:*****:						
cpe:2.3:a:samba:samba:4.0.14:*****:						

cpe:2.3:a:samba:samba:4.0.15:*****:
cpe:2.3:a:samba:samba:4.0.16:*****:
cpe:2.3:a:samba:samba:4.0.17:*****:
cpe:2.3:a:samba:samba:4.0.18:*****:
cpe:2.3:a:samba:samba:4.0.19:*****:
cpe:2.3:a:samba:samba:4.0.2:*****:
cpe:2.3:a:samba:samba:4.0.20:*****:
cpe:2.3:a:samba:samba:4.0.21:*****:
cpe:2.3:a:samba:samba:4.0.22:*****:
cpe:2.3:a:samba:samba:4.0.23:*****:
cpe:2.3:a:samba:samba:4.0.24:*****:
cpe:2.3:a:samba:samba:4.0.3:*****:
cpe:2.3:a:samba:samba:4.0.4:*****:
cpe:2.3:a:samba:samba:4.0.5:*****:
cpe:2.3:a:samba:samba:4.0.6:*****:
cpe:2.3:a:samba:samba:4.0.7:*****:
cpe:2.3:a:samba:samba:4.0.8:*****:
cpe:2.3:a:samba:samba:4.0.9:*****:
cpe:2.3:a:samba:samba:4.1.0:*****:
cpe:2.3:a:samba:samba:4.1.1:*****:
cpe:2.3:a:samba:samba:4.1.10:*****:
cpe:2.3:a:samba:samba:4.1.11:*****:
cpe:2.3:a:samba:samba:4.1.12:*****:
cpe:2.3:a:samba:samba:4.1.13:*****:
cpe:2.3:a:samba:samba:4.1.14:*****:
cpe:2.3:a:samba:samba:4.1.15:*****:
cpe:2.3:a:samba:samba:4.1.16:*****:
cpe:2.3:a:samba:samba:4.1.17:*****:
cpe:2.3:a:samba:samba:4.1.18:*****:

cpe:2.3:a:samba:samba:4.1.18:*****:
cpe:2.3:a:samba:samba:4.1.19:*****:
cpe:2.3:a:samba:samba:4.1.2:*****:
cpe:2.3:a:samba:samba:4.1.20:*****:
cpe:2.3:a:samba:samba:4.1.21:*****:
cpe:2.3:a:samba:samba:4.1.3:*****:
cpe:2.3:a:samba:samba:4.1.4:*****:
cpe:2.3:a:samba:samba:4.1.5:*****:
cpe:2.3:a:samba:samba:4.1.6:*****:
cpe:2.3:a:samba:samba:4.1.7:*****:
cpe:2.3:a:samba:samba:4.1.8:*****:
cpe:2.3:a:samba:samba:4.1.9:*****:
cpe:2.3:a:samba:samba:4.2.0:*****:
cpe:2.3:a:samba:samba:4.2.1:*****:
cpe:2.3:a:samba:samba:4.2.2:*****:
cpe:2.3:a:samba:samba:4.2.3:*****:
cpe:2.3:a:samba:samba:4.2.4:*****:
cpe:2.3:a:samba:samba:4.2.5:*****:
cpe:2.3:a:samba:samba:4.2.6:*****:
cpe:2.3:a:samba:samba:4.3.0:*****:
cpe:2.3:a:samba:samba:4.3.1:*****:
cpe:2.3:a:samba:samba:4.3.2:*****:
cpe:2.3:a:samba:samba:4.0.0:*****:
cpe:2.3:a:samba:samba:4.0.1:*****:
cpe:2.3:a:samba:samba:4.0.10:*****:
cpe:2.3:a:samba:samba:4.0.11:*****:
cpe:2.3:a:samba:samba:4.0.12:*****:
cpe:2.3:a:samba:samba:4.0.13:*****:
cpe:2.3:a:samba:samba:4.0.14:*****:

cpe:2.3:a:samba:samba:4.0.15:*****:
cpe:2.3:a:samba:samba:4.0.16:*****:
cpe:2.3:a:samba:samba:4.0.17:*****:
cpe:2.3:a:samba:samba:4.0.18:*****:
cpe:2.3:a:samba:samba:4.0.19:*****:
cpe:2.3:a:samba:samba:4.0.2:*****:
cpe:2.3:a:samba:samba:4.0.20:*****:
cpe:2.3:a:samba:samba:4.0.21:*****:
cpe:2.3:a:samba:samba:4.0.22:*****:
cpe:2.3:a:samba:samba:4.0.23:*****:
cpe:2.3:a:samba:samba:4.0.24:*****:
cpe:2.3:a:samba:samba:4.0.3:*****:
cpe:2.3:a:samba:samba:4.0.4:*****:
cpe:2.3:a:samba:samba:4.0.5:*****:
cpe:2.3:a:samba:samba:4.0.6:*****:
cpe:2.3:a:samba:samba:4.0.7:*****:
cpe:2.3:a:samba:samba:4.0.8:*****:
cpe:2.3:a:samba:samba:4.0.9:*****:
cpe:2.3:a:samba:samba:4.1.0:*****:
cpe:2.3:a:samba:samba:4.1.1:*****:
cpe:2.3:a:samba:samba:4.1.10:*****:
cpe:2.3:a:samba:samba:4.1.11:*****:
cpe:2.3:a:samba:samba:4.1.12:*****:
cpe:2.3:a:samba:samba:4.1.13:*****:
cpe:2.3:a:samba:samba:4.1.14:*****:
cpe:2.3:a:samba:samba:4.1.15:*****:
cpe:2.3:a:samba:samba:4.1.16:*****:
cpe:2.3:a:samba:samba:4.1.17:*****:

cpe:2.3:a:samba:samba:4.1.18:*****:
cpe:2.3:a:samba:samba:4.1.19:*****:
cpe:2.3:a:samba:samba:4.1.2:*****:
cpe:2.3:a:samba:samba:4.1.20:*****:
cpe:2.3:a:samba:samba:4.1.21:*****:
cpe:2.3:a:samba:samba:4.1.3:*****:
cpe:2.3:a:samba:samba:4.1.4:*****:
cpe:2.3:a:samba:samba:4.1.5:*****:
cpe:2.3:a:samba:samba:4.1.6:*****:
cpe:2.3:a:samba:samba:4.1.7:*****:
cpe:2.3:a:samba:samba:4.1.8:*****:
cpe:2.3:a:samba:samba:4.1.9:*****:
cpe:2.3:a:samba:samba:4.2.0:*****:
cpe:2.3:a:samba:samba:4.2.1:*****:
cpe:2.3:a:samba:samba:4.2.2:*****:
cpe:2.3:a:samba:samba:4.2.3:*****:
cpe:2.3:a:samba:samba:4.2.4:*****:
cpe:2.3:a:samba:samba:4.2.5:*****:
cpe:2.3:a:samba:samba:4.2.6:*****:
cpe:2.3:a:samba:samba:4.3.0:*****:
cpe:2.3:a:samba:samba:4.3.1:*****:
cpe:2.3:a:samba:samba:4.3.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)