



# CVE-2018-16851

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-16851
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-11-28 14:29:00 UTC
<b>Updated</b>	2022-08-29 20:03:00 UTC
<b>Description</b>	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	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
1646377 – (CVE-2018-16851) CVE-2018-16851 samba: NULL pointer de-reference in Samba AD DC LDAP server	CONFIRM	<a href="#">bugzilla.re</a>
Samba - Security Announcement Archive	CONFIRM	<a href="#">www.samb</a>
Samba CVE-2018-16851 Remote Denial of Service Vulnerability	BID	<a href="#">www.secu</a>
[SECURITY] [DLA 1607-1] samba security update	MLIST	<a href="#">lists.debia</a>
Debian -- Security Information -- DSA-4345-1 samba	DEBIAN	<a href="#">www.debia</a>
USN-3827-1: Samba vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu</a>
USN-3827-2: Samba vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubuntu</a>
November 2018 Samba Vulnerabilities in NetApp StorageGRID Products   NetApp Product Security	CONFIRM	<a href="#">security.ne</a>
Samba: Multiple vulnerabilities (GLSA 202003-52) — Gentoo security	GENTOO	<a href="#">security.ge</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gc</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[500637](#) Alpine Linux Security Update for samba

[504401](#) Alpine Linux Security Update for samba

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)