



CVE-2015-5252

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

Last Modified on: 08/29/2022 08:26:00 PM UTC

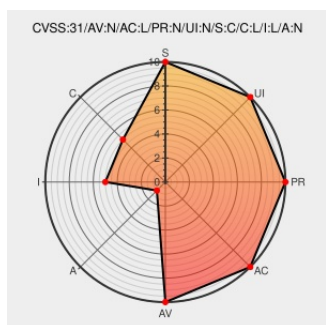
CVE-2015-5252

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share.

CVE-2015-5252 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
USN-2855-1: Samba vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2855-1
Document Display HPE Support Center	h20566.www2.hp.com text/html	CONFIRM h20566.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?

[security-announce] SUSE-SU-2015:2304-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:2304
Samba: Multiple vulnerabilities (GLSA 201612-47) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201612-47
Bug 1290288 – CVE-2015-5252 samba: Insufficient symlink verification in smbd	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1290288
[SECURITY] Fedora 23 Update: samba-4.3.3-0.fc23	lists.fedoraproject.org text/html	 FEDORA FEDORA-2015-b36076d32e
[security-announce] SUSE-SU-2016:0032-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:0032
[security-announce] openSUSE-SU-2016:1107-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:1107
[security-announce] SUSE-SU-2016:1105-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:1105
[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
[security-announce] openSUSE-SU-2015:2354-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2354
Samba CVE-2015-5252 Symlink Vulnerability	cve.report (archive) text/html	 BID 79733
Samba - Security Announcement Archive	Exploit Vendor Advisory www.samba.org text/html	 CONFIRM www.samba.org/samba/security/CVE-2015-5252.html
[security-announce] openSUSE-SU-2015:2356-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2356
[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=4278ef25f64d5fdbf432ff1534e275416ec9561e
Debian -- Security Information -- DSA-3433-1 samba	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3433

[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] Fedora 22 Update: samba-4.2.7-0.fc22

lists.fedoraproject.org
text/html

 FEDORA FEDORA-2015-0e0879cc8a

Oracle Solaris Bulletin - January 2016

www.oracle.com
text/html

 CONFIRM
www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html

[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
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Samba	Samba	All	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	4.1.14	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	4.1.14	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:o:canonical:ubuntu_linux:12.04:*:*:*:-:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:
```

```
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:samba:samba:*:*:*:*:*:*:*:
```

```
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:*****:
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:*****:

Урб.З.О.А.Замнаа.Замнаа.Т.У.У.

```
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.report](#) 2023   |

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](#)