



# CVE-2019-10218

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

## Summary

<b>CVE</b>	CVE-2019-10218
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-06 10:15:00 UTC
<b>Updated</b>	2023-11-07 03:02:00 UTC
<b>Description</b>	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	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>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	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] Fedora 30 Update: samba-4.10.10-0.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fec</a>
[SECURITY] Fedora 31 Update: samba-4.11.2-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fec</a>
[SECURITY] [DLA 3563-1] samba security update	MLIST	<a href="#">lists.de</a>
[SECURITY] Fedora 29 Update: samba-4.9.15-0.fc29 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fec</a>
[SECURITY] Fedora 29 Update: samba-4.9.15-0.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fec</a>
Synology Inc.	CONFIRM	<a href="#">www.sy</a>
Samba - Security Announcement Archive	MISC	<a href="#">www.sa</a>
[security-announce] openSUSE-SU-2019:2458-1: important: Security update	SUSE	<a href="#">lists.op</a>

[SECURITY] Fedora 30 Update: samba-4.10.10-0.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fec</a>
[SECURITY] Fedora 31 Update: samba-4.11.2-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fec</a>
[SECURITY] [DLA 2668-1] samba security update	MLIST	<a href="#">lists.de</a>
1763137 – (CVE-2019-10218) CVE-2019-10218 samba: smb client vulnerable to filenames containing path separators	CONFIRM	<a href="#">bugzilla</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [178607](#) Debian Security Update for samba (DLA 2668-1)
- [296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)
- [377231](#) Alibaba Cloud Linux Security Update for samba (ALINUX2-SA-2020:0079)
- [377403](#) Alibaba Cloud Linux Security Update for samba (ALINUX3-SA-2021:0077)
- [500622](#) Alpine Linux Security Update for samba
- [504384](#) Alpine Linux Security Update for samba
- [6000093](#) Debian Security Update for samba (DLA 3563-1)
- [671072](#) EulerOS Security Update for samba (EulerOS-SA-2019-2547)

© [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](#)