

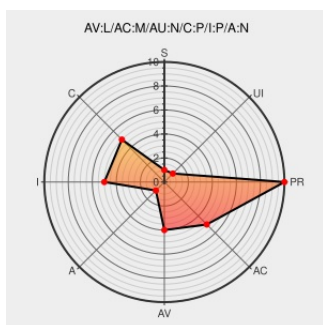


# CVE-2011-1585

Published on: 06/08/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:17:00 AM UTC

## CVE-2011-1585

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

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

The `cifs_find_smb_ses` function in `fs/cifs/connect.c` in the Linux kernel before 2.6.36 does not properly determine the associations between users and sessions, which allows local users to bypass CIFS share authentication by leveraging a mount of a share by a different user.

CVE-2011-1585 has been assigned by [secalert@redhat.com](mailto:secalert@redhat.com) to track the vulnerability

CVSS2 Score: **3.3 - LOW**

Access  
Vector

LOCAL

Access  
Complexity

MEDIUM

Authentication

NONE

Confidentiality  
Impact

PARTIAL

Integrity  
Impact

PARTIAL

Availability  
Impact

NONE

## CVE References

Description

Tags

Link

kernel/git/torvalds/linux.git -  
Linux kernel source tree

[Exploit](#)  
[Patch](#)  
[web.archive.org](#)  
[text/html](#)  
[Inactive Link](#) [Not Archived](#)

MISC [git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=4ff67b720c02c36e54d55b88c2931879b7db1cd2](https://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=4ff67b720c02c36e54d55b88c2931879b7db1cd2)

[security-announce] SUSE-  
SU-2015:0812-1:  
important: Security update  
for

[Mailing List](#)  
[Third Party Advisory](#)  
[lists.opensuse.org](#)  
[text/html](#)

SUSE [SUSE-SU-2015:0812](#)

697394 – (CVE-2011-  
1585) CVE-2011-1585  
kernel: cifs session reuse

[Issue Tracking](#)  
[Patch](#)  
[Third Party Advisory](#)  
[bugzilla.redhat.com](#)  
[text/html](#)

CONFIRM [bugzilla.redhat.com/show\\_bug.cgi?id=697394](https://bugzilla.redhat.com/show_bug.cgi?id=697394)

cifs: clean up  
cifs\_find\_smb\_ses (try #2)  
· torvalds/linux@4ff67b7 ·  
GitHub

Exploit

Patch

Third Party Advisory

github.com

text/html

**CONFIRM**  
github.com/torvalds/linux/commit/4ff67b720c02c36e54d55b88c2931879b7db1cd2

404 Not Found

Release Notes

Third Party Advisory

ftp.osuosl.org

text/plain

Inactive Link

Not Archived

**CONFIRM** ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36

oss-security - Re: CVE  
Request: cifs session  
reuse

Mailing List

Third Party Advisory

www.openwall.com

text/html

**MLIST** [oss-security] 20110415 Re: CVE Request: cifs session reuse

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](mailto: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                                          | Linux  | Linux Kernel                 | All     | All    | All     | All      |
| Operating System                                          | Linux  | Linux Kernel                 | All     | All    | All     | All      |
| Operating System                                          | Suse   | Suse Linux Enterprise Server | 10      | sp4    | All     | All      |
| Operating System                                          | Suse   | Suse Linux Enterprise Server | 10      | sp4    | All     | All      |
| cpe:2.3:o:linux:linux_kernel:*****:                       |        |                              |         |        |         |          |
| cpe:2.3:o:linux:linux_kernel:*****:                       |        |                              |         |        |         |          |
| cpe:2.3:o:suse:suse_linux_enterprise_server:10:sp4:*****: |        |                              |         |        |         |          |
| cpe:2.3:o:suse:suse_linux_enterprise_server:10:sp4:*****: |        |                              |         |        |         |          |

No vendor comments have been submitted for this CVE

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](#)