

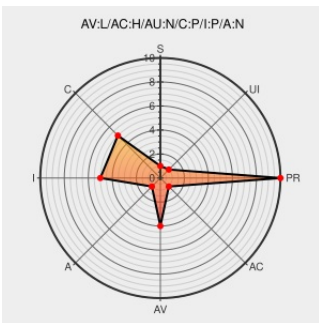


# CVE-2013-2207

Published on: 10/09/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:25 AM UTC

## CVE-2013-2207

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

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

pt\_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, which allows local users to change the permission on the files and obtain access to arbitrary pseudo-terminals by leveraging a FUSE file system.

CVE-2013-2207 has been assigned by [secalert@redhat.com](mailto:secalert@redhat.com) to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access  
Vector

LOCAL

Access  
Complexity

HIGH

Authentication

NONE

Confidentiality  
Impact

PARTIAL

Integrity  
Impact

PARTIAL

Availability  
Impact

NONE

## CVE References

Description

Tags

Link

[security-announce] SUSE-SU-2016:0470-1: important: Security update for

[lists.opensuse.org](#)  
text/html

[SUSE SUSE-SU-2016:0470](#)

USN-2985-2: GNU C Library regression | Ubuntu

[www.ubuntu.com](#)  
text/html

[UBUNTU USN-2985-2](#)

David Miller - The GNU C Library version 2.18 is now available

[sourceware.org](#)  
text/html

[MLIST \[libc-alpha\] 20130812 The GNU C Library version 2.18 is now available](#)

15755 – (CVE-2013-2207) CVE-2013-2207: pt\_chown tricked into granting access to another users pseudo-terminal

[Patch](#)  
[sourceware.org](#)  
text/html

[CONFIRM](#)  
[sourceware.org/bugzilla/show\\_bug.cgi?id=15755](#)

About Secunia Research | Flexera

[secunia.com](#)  
[Deprecated Link](#)  
text/plain

[SECUNIA 55113](#)

|                                                                                                                                                                |                                                                                                              |                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| USN-2985-1: GNU C Library vulnerabilities   Ubuntu                                                                                                             | <a href="http://www.ubuntu.com/text/html">www.ubuntu.com</a><br>text/html                                    |  UBUNTU USN-2985-1                                                                                                     |
| Support / Security / Advisories // MDVSA-2013:283   Mandriva                                                                                                   | <a href="http://www.mandriva.com/text/html">www.mandriva.com</a><br>text/html                                |  MANDRIVA MDVSA-2013:283                                                                                               |
| Gentoo Security                                                                                                                                                | <a href="http://security.gentoo.org/text/html">security.gentoo.org</a><br>text/html                          |  GENTOO GLSA-201503-04                                                                                                 |
| 976408 – (CVE-2013-2207) CVE-2013-2207 glibc (pt_chown): Improper pseudotty ownership and permissions changes when granting access to the slave pseudoterminal | <a href="#">Patch</a><br><a href="http://bugzilla.redhat.com/text/html">bugzilla.redhat.com</a><br>text/html |  CONFIRM<br><a href="http://bugzilla.redhat.com/show_bug.cgi?id=976408">bugzilla.redhat.com/show_bug.cgi?id=976408</a> |
| [security-announce] SUSE-SU-2015:1424-1: important: Security update for                                                                                        | <a href="http://lists.opensuse.org/text/html">lists.opensuse.org</a><br>text/html                            |  SUSE SUSE-SU-2015:1424                                                                                                |

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 | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a> | 18      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a> | 19      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a> | 18      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a> | 19      | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.0     | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.0.1   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.0.2   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.0.3   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.0.4   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.0.5   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.0.6   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.1     | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.1.1   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.1.1.6 | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.1.2   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.1.3   | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Glibc</a>  | 2.1.9   | All    | All     | All      |

|             |                     |                       |         |     |     |     |
|-------------|---------------------|-----------------------|---------|-----|-----|-----|
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.10.1  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11.1  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11.2  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11.3  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.12.1  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.12.2  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.13    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.14    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.14.1  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.15    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.16    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.0     | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.0.1   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.0.2   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.0.3   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.0.4   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.0.5   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.0.6   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.1     | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.1.1   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.1.1.6 | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.1.2   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.1.3   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.1.9   | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.10.1  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11.1  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11.2  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.11.3  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.12.1  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.12.2  | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.13    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.14    | All | All | All |
| Application | <a href="#">Gnu</a> | <a href="#">Glibc</a> | 2.14.1  | All | All | All |

|                                          |     |       |      |     |     |     |
|------------------------------------------|-----|-------|------|-----|-----|-----|
| Application                              | Gnu | Glibc | 2.15 | All | All | All |
| Application                              | Gnu | Glibc | 2.16 | All | All | All |
| Application                              | Gnu | Glibc | All  | All | All | All |
| cpe:2.3:o:fedoraproject:fedora:18:*****: |     |       |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:19:*****: |     |       |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:18:*****: |     |       |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:19:*****: |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.0:*****:           |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.0.1:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.0.2:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.0.3:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.0.4:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.0.5:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.0.6:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.1:*****:           |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.1.1:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.1.1.6:*****:       |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.1.2:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.1.3:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.1.9:*****:         |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.10.1:*****:        |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.11:*****:          |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.11.1:*****:        |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.11.2:*****:        |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.11.3:*****:        |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.12.1:*****:        |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.12.2:*****:        |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.13:*****:          |     |       |      |     |     |     |
| cpe:2.3:a:gnu:glibc:2.14:*****:          |     |       |      |     |     |     |

|                                    |
|------------------------------------|
| cpe:2.3:a:gnu:glibc:2.14.1:*****:  |
| cpe:2.3:a:gnu:glibc:2.15:*****:    |
| cpe:2.3:a:gnu:glibc:2.16:*****:    |
| cpe:2.3:a:gnu:glibc:2.0:*****:     |
| cpe:2.3:a:gnu:glibc:2.0.1:*****:   |
| cpe:2.3:a:gnu:glibc:2.0.2:*****:   |
| cpe:2.3:a:gnu:glibc:2.0.3:*****:   |
| cpe:2.3:a:gnu:glibc:2.0.4:*****:   |
| cpe:2.3:a:gnu:glibc:2.0.5:*****:   |
| cpe:2.3:a:gnu:glibc:2.0.6:*****:   |
| cpe:2.3:a:gnu:glibc:2.1:*****:     |
| cpe:2.3:a:gnu:glibc:2.1.1:*****:   |
| cpe:2.3:a:gnu:glibc:2.1.1.6:*****: |
| cpe:2.3:a:gnu:glibc:2.1.2:*****:   |
| cpe:2.3:a:gnu:glibc:2.1.3:*****:   |
| cpe:2.3:a:gnu:glibc:2.1.9:*****:   |
| cpe:2.3:a:gnu:glibc:2.10.1:*****:  |
| cpe:2.3:a:gnu:glibc:2.11:*****:    |
| cpe:2.3:a:gnu:glibc:2.11.1:*****:  |
| cpe:2.3:a:gnu:glibc:2.11.2:*****:  |
| cpe:2.3:a:gnu:glibc:2.11.3:*****:  |
| cpe:2.3:a:gnu:glibc:2.12.1:*****:  |
| cpe:2.3:a:gnu:glibc:2.12.2:*****:  |
| cpe:2.3:a:gnu:glibc:2.13:*****:    |
| cpe:2.3:a:gnu:glibc:2.14:*****:    |
| cpe:2.3:a:gnu:glibc:2.14.1:*****:  |
| cpe:2.3:a:gnu:glibc:2.15:*****:    |
| cpe:2.3:a:gnu:glibc:2.16:*****:    |
| cpe:2.3:a:gnu:glibc:*****:         |

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](#)