



# CVE-2009-4135

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

## Summary

<b>CVE</b>	CVE-2009-4135
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-12-11 16:30:00 UTC
<b>Updated</b>	2023-02-13 02:20:00 UTC
<b>Description</b>	The distcheck rule in dist-check.mk in GNU coreutils 5.2.1 through 8.1 allows local users to gain privileges via a symlink att...

## Risk And Classification

### Problem Types: CWE-59

## 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>	10.04	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>	10.04	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="#">Fedoraproject</a>	<a href="#">Fedora</a>	11	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	12	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	11	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	12	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	5.2.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	5.91	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	5.92	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	5.93	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	5.94	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	5.95	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	5.96	All	All	All

Application	Gnu	Coreutils	5.97	All	All	All
Application	Gnu	Coreutils	6.10	All	All	All
Application	Gnu	Coreutils	6.11	All	All	All
Application	Gnu	Coreutils	6.12	All	All	All
Application	Gnu	Coreutils	6.2	All	All	All
Application	Gnu	Coreutils	6.3	All	All	All
Application	Gnu	Coreutils	6.4	All	All	All
Application	Gnu	Coreutils	6.5	All	All	All
Application	Gnu	Coreutils	6.6	All	All	All
Application	Gnu	Coreutils	6.7	All	All	All
Application	Gnu	Coreutils	6.8	All	All	All
Application	Gnu	Coreutils	6.9	All	All	All
Application	Gnu	Coreutils	7.1	All	All	All
Application	Gnu	Coreutils	7.2	All	All	All
Application	Gnu	Coreutils	7.3	All	All	All
Application	Gnu	Coreutils	7.4	All	All	All
Application	Gnu	Coreutils	7.5	All	All	All
Application	Gnu	Coreutils	7.6	All	All	All
Application	Gnu	Coreutils	8.1	All	All	All
Application	Gnu	Coreutils	5.2.1	All	All	All
Application	Gnu	Coreutils	5.91	All	All	All
Application	Gnu	Coreutils	5.92	All	All	All
Application	Gnu	Coreutils	5.93	All	All	All
Application	Gnu	Coreutils	5.94	All	All	All
Application	Gnu	Coreutils	5.95	All	All	All
Application	Gnu	Coreutils	5.96	All	All	All
Application	Gnu	Coreutils	5.97	All	All	All
Application	Gnu	Coreutils	6.10	All	All	All
Application	Gnu	Coreutils	6.11	All	All	All
Application	Gnu	Coreutils	6.12	All	All	All
Application	Gnu	Coreutils	6.2	All	All	All
Application	Gnu	Coreutils	6.3	All	All	All
Application	Gnu	Coreutils	6.4	All	All	All
Application	Gnu	Coreutils	6.5	All	All	All
Application	Gnu	Coreutils	6.6	All	All	All

Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	6.7	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	6.8	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	6.9	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	7.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	7.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	7.3	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	7.4	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	7.5	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	7.6	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Coreutils</a>	8.1	All	All	All

## References

### Reference

[USN-2473-1: coreutils vulnerabilities | Ubuntu](#)

[GNU Core Utilities "distcheck" Insecure Temporary Directory Security Issue - Secunia Advisories - Vulnerability Information - Secunia.com](#)

['Re: \[oss-security\] CVE Request -- coreutils -- unsafe temporary' - MARC](#)

[oss-security - CVE Request -- coreutils -- unsafe temporary directory location use](#)

[\[SECURITY\] Fedora 11 Update: coreutils-7.2-5.fc11](#)

60853

[\[SECURITY\] Fedora 12 Update: coreutils-7.6-8.fc12](#)

[Re: build: distcheck: do not leave a \\$TMPDIR/coreutils directory behind](#)

[IBM X-Force Exchange](#)

[Fedora update for coreutils - Secunia.com](#)

[\[PATCH\] doc: NEWS: mention the "make distcheck" vulnerability](#)

[Re: build: distcheck: do not leave a \\$TMPDIR/coreutils directory behind](#)

[\[PATCH\] doc: NEWS: mention the "make distcheck" vulnerability](#)

[Security Advisory SA62226 - Ubuntu update for coreutils - Secunia](#)

[coreutils.git - GNU coreutils](#)

[Bug 545439 – CVE-2009-4135 coreutils: Unsafe temporary directory use in "distcheck" rule](#)

[GNU Coreutils Insecure Temporary File Creation Vulnerability](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

## Vendor Comments And Credit

Organization	Published	Contributor	Statement
--------------	-----------	-------------	-----------

There are currently no legacy QID mappings associated with this CVE.

© [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](#)