



# CVE-2014-3537

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2014-3537
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-07-23 14:55:00 UTC
<b>Updated</b>	2023-02-13 00:40:00 UTC
<b>Description</b>	The web interface in CUPS before 1.7.4 allows local users in the lp group to read arbitrary files via a symlink attack on a file

## Risk And Classification

### Problem Types: CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7	rc1	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.0	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.1	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.1	b1	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.2	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7	rc1	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.0	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.1	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.1	b1	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	1.7.2	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Cups</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	10.04	-	lts	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	-	lts	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	-	lts	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	-	lts	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>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All

## References

Reference	Source	Link
CVE-2014-3537: Insufficient checking leads to privilege escalation · Issue #4450 · apple/cups · GitHub	CONFIRM	<a href="http://www.cups.org">www.cups.org</a>
USN-2293-1: CUPS vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
About the security content of OS X Yosemite v10.10 - Apple Support	CONFIRM	<a href="http://support.apple.com">support.apple.com</a>
Red Hat Customer Portal	MISC	<a href="http://access.redhat.com">access.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
Support / Security / Advisories // MDVSA-2015:108   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Article #724: CUPS 1.7.4 - CUPS.org	CONFIRM	<a href="http://www.cups.org">www.cups.org</a>
Bug 1115576 – CVE-2014-3537 cups: insufficient checking leads to privilege escalation	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
CUPS Web Interface CVE-2014-3537 Local Privilege Escalation Vulnerability	BID	<a href="http://www.securityfocus.co">www.securityfocus.co</a>
NEOHAPSIS - Peace of Mind Through Integrity and Insight	APPLE	<a href="http://archives.neohapsis.co">archives.neohapsis.co</a>
CUPS RSS Web Interface Lets Local Users View Privileged Files - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.c">www.securitytracker.c</a>
Red Hat Customer Portal	MISC	<a href="http://access.redhat.com">access.redhat.com</a>
Security Advisory SA60273 - Ubuntu update for cups - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Security Advisory SA60787 - SUSE update for cups - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[SECURITY] Fedora 20 Update: cups-1.7.4-1.fc20	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>
Mageia Advisory: MGASA-2014-0313 - Updated cups packages fix security vulnerability	CONFIRM	<a href="http://advisories.mageia.org">advisories.mageia.org</a>
<a href="http://access.redhat.com">access.redhat.com</a>   CVE-2014-3537	MISC	<a href="http://access.redhat.com">access.redhat.com</a>
About Secunia Research   Flexera	SECUNIA	<a href="http://secunia.com">secunia.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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](#).

