



# CVE-2015-1038

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

## Summary

<b>CVE</b>	CVE-2015-1038
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-01-21 18:59:00 UTC
<b>Updated</b>	2017-09-08 01:29:00 UTC
<b>Description</b>	p7zip 9.20.1 allows remote attackers to write to arbitrary files via a symlink attack in an archive.

## Risk And Classification

### Problem Types: CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">7-zip</a>	<a href="#">P7zip</a>	9.20.1	All	All	All
Application	<a href="#">7-zip</a>	<a href="#">P7zip</a>	9.20.1	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	22	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	10.0	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	11.2	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	10.0	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Solaris</a>	11.2	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 22 Update: p7zip-15.09-4.fc22	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Debian -- Security Information -- DSA-3289-1 p7zip	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
openSUSE-SU-2015:1162-1: moderate: Security update for p7zip	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
#774660 - p7zip: CVE-2015-1038: Directory traversal through symlinks - Debian Bug report logs	MISC	<a href="https://bugs.debian.org">bugs.debian.org</a>
oss-security: Re: CVE request for directory traversal flaw in p7zip	MISC	<a href="http://www.openwall.com">www.openwall.com</a>

oss-security - Re: CVE request for directory traversal flaw in p7zip	MISC	<a href="http://www.openwall.com">www.openwall.com</a>
Oracle Solaris Third Party Bulletin - July 2015	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>
Bug 1179505 – CVE-2015-1038 p7zip: directory traversal vulnerability	MISC	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
p7zip Symlink Directory Traversal Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
[SECURITY] Fedora 23 Update: p7zip-15.09-4.fc23	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org/cve). This site includes MITRE data granted under the following [license](http://www.mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)