



# CVE-2008-4636

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

## Summary

<b>CVE</b>	CVE-2008-4636
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-11-27 00:30:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	yast2-backup 2.14.2 through 2.16.6 on SUSE Linux and Novell Linux allows local users to gain privileges via shell metacha

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Novell	Opensuse	All	All	All	All
Operating System	Novell	Opensuse	All	All	All	All
Operating System	Novell	Suse Linux	All	All	All	All
Operating System	Novell	Suse Linux	10	All	desktop	All
Operating System	Novell	Suse Linux	10	All	server	All
Operating System	Novell	Suse Linux	10.0	All	All	All
Operating System	Novell	Suse Linux	10.1	All	All	All
Operating System	Novell	Suse Linux	9	All	server	All
Operating System	Novell	Suse Linux	9.3	All	pro	All
Operating System	Novell	Suse Linux	All	All	All	All
Operating System	Novell	Suse Linux	10	All	desktop	All
Operating System	Novell	Suse Linux	10	All	server	All
Operating System	Novell	Suse Linux	10.0	All	All	All
Operating System	Novell	Suse Linux	10.1	All	All	All
Operating System	Novell	Suse Linux	9	All	server	All
Operating System	Novell	Suse Linux	9.3	All	pro	All
Operating System	Novell	Suse Linux Enterprise Server	All	All	All	All

Operating System	Novell	Suse Linux Enterprise Server	9	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	9	All	All	All
Operating System	Opensuse	Opensuse	All	All	All	All
Operating System	Opensuse	Opensuse	10.2	All	All	All
Operating System	Opensuse	Opensuse	10.3	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	All	All	All	All
Operating System	Opensuse	Opensuse	10.2	All	All	All
Operating System	Opensuse	Opensuse	10.3	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Suse	Yast2-backup	2.14.2	All	All	All
Operating System	Suse	Yast2-backup	2.14.2	All	All	All
Operating System	Suse	Yast2-backup	All	All	All	All

## References

Reference	Source	Link	Tags
[security-announce] SUSE Security Announcement: yast2-backup (SUSE-SA:2050284)	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Patch
IBM X-Force Exchange	OSVDB	<a href="https://osvdb.org">osvdb.org</a>	
SuSE YaST2 Backup File Name Local Arbitrary Shell Command Injection Vulnerability	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
SUSE update for yast2-backup - Secunia.com	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Patch
CVE Program record	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Patch
NVD vulnerability detail	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canor
	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canor

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

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