



CVE-2009-4411

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

Summary

CVE	CVE-2009-4411
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-12-24 16:30:00 UTC
Updated	2017-08-17 01:31:00 UTC
Description	The (1) setfacl and (2) getfacl commands in XFS acl 2.2.47, when running in recursive (-R) mode, follow symbolic links eve

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xfs	Acl	2.2.47	All	All	All
Application	Xfs	Acl	2.2.47	All	All	All

References

Reference	Source	Link
XFS Acl Recursive Symlink Processing Security Issue - Secunia.com	SECUNIA	secunia.com
XFS ACL 'setfacl' and 'getfacl' Symbolic Link Handling Security Bypass Vulnerability	BID	www.securityfocus.com
#499076 - CVE-2009-4411: Physical walk no longer ignores all symlinks - Debian Bug report logs	CONFIRM	bugs.debian.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:002	SUSE	lists.opensuse.org
Bug 790 – getfacl 2.2.47 follows symlinks, even without -L	CONFIRM	oss.sgi.com
SUSE Update for Multiple Packages - Secunia.com	SECUNIA	secunia.com
acl.git - acl	CONFIRM	git.savannah.gnu.org
oss-security - CVE request: acl 2.2.47 always follows symlinks	MLIST	www.openwall.com
61302	OSVDB	osvdb.org
Support / Security / Advisories // MDVSA-2009:345 Mandriva	MANDRIVA	www.mandriva.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.
CVE Program record	CVE.ORG	www.cve.org

NVD vulnerability detailNVDnvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2010-01-21	Tomas Hoger	Not vulnerable. This issue did not affect the versions of acl as shipped with Red Hat Enterprise

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)