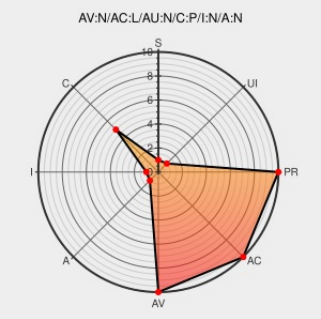
CVE-2005-3623

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

CVE-2005-3623

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

nfs2acl.c in the Linux kernel 2.6.14.4 does not check for MAY_SATTR privilege before setting access controls (ACL) on files on exported NFS filesystems, which allows remote attackers to bypass ACLs for readonly mounted NFS filesystems.

CVE-2005-3623 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Linux Kernel NFS ACL Access Control Bypass Vulnerability	cve.report (archive) text/html	BID 16570
ASA-2006-200 (RHSA-2006-0575)	support.avaya.com text/html	CONFIRM support.avaya.com/elmodocs2/security/ASA-2006-200.htm
LKML: Greg Kroah-Hartman: [patch 19/19] setting ACLs on readonly mounted NFS filesystems (CVE-2005-3623)	Patch lkml.org text/xml	MISC lkml.org/lkml/2005/12/23/171
Security Announcement	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2006:006
SuSE Security announcements: [suse-security-announce] SUSE	Patch	SUSE SUSE-SA:2006:012

Security Announcement: kernel various security problems (SUSE-SA:2006:012)	web.archive.org text/html Inactive Link Not Archived	
rhn.redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2006:0575
Secunia - Advisories - SUSE update for kernel	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19038
Red Hat update for kernel - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 21465
SUSE update for kernel - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 18788
Avaya Products Linux Kernel Multiple Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22417
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11707

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.14.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.14.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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