



CVE-2010-2943

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2010-2943
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-09-30 15:00:00 UTC
Updated	2023-02-13 04:21:00 UTC
Description	The xfs implementation in the Linux kernel before 2.6.35 does not look up inode allocation btrees before reading inode buff

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Aura Communication Manager	5.2	All	All	All
Application	Avaya	Aura Communication Manager	5.2	All	All	All
Application	Avaya	Aura Presence Services	6.0	All	All	All
Application	Avaya	Aura Presence Services	6.1	All	All	All
Application	Avaya	Aura Presence Services	6.1.1	All	All	All
Application	Avaya	Aura Presence Services	6.0	All	All	All
Application	Avaya	Aura Presence Services	6.1	All	All	All
Application	Avaya	Aura Presence Services	6.1.1	All	All	All
Application	Avaya	Aura Session Manager	1.1	All	All	All
Application	Avaya	Aura Session Manager	5.2	All	All	All
Application	Avaya	Aura Session Manager	6.0	All	All	All
Application	Avaya	Aura Session Manager	1.1	All	All	All
Application	Avaya	Aura Session Manager	5.2	All	All	All
Application	Avaya	Aura Session Manager	6.0	All	All	All
Application	Avaya	Aura System Manager	5.2	All	All	All
Application	Avaya	Aura System Manager	6.0	All	All	All
Application	Avaya	Aura System Manager	6.1	All	All	All

Application	Avaya	Aura System Manager	6.1.1	All	All	All
Application	Avaya	Aura System Manager	5.2	All	All	All
Application	Avaya	Aura System Manager	6.0	All	All	All
Application	Avaya	Aura System Manager	6.1	All	All	All
Application	Avaya	Aura System Manager	6.1.1	All	All	All
Application	Avaya	Aura System Platform	1.1	All	All	All
Application	Avaya	Aura System Platform	6.0	-	All	All
Application	Avaya	Aura System Platform	6.0	sp1	All	All
Application	Avaya	Aura System Platform	1.1	All	All	All
Application	Avaya	Aura System Platform	6.0	-	All	All
Application	Avaya	Aura System Platform	6.0	sp1	All	All
Application	Avaya	Aura Voice Portal	5.0	All	All	All
Application	Avaya	Aura Voice Portal	5.1	-	All	All
Application	Avaya	Aura Voice Portal	5.1	sp1	All	All
Application	Avaya	Aura Voice Portal	5.0	All	All	All
Application	Avaya	Aura Voice Portal	5.1	-	All	All
Application	Avaya	Aura Voice Portal	5.1	sp1	All	All
Application	Avaya	Iq	5.0	All	All	All
Application	Avaya	Iq	5.1	All	All	All
Application	Avaya	Iq	5.0	All	All	All
Application	Avaya	Iq	5.1	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.1	All	All	All
Operating System	Vmware	Esx	4.0	All	All	All
Operating System	Vmware	Esx	4.1	All	All	All

References

Reference	Source	Link	Tags
404: File not found	CONFIRM	www.kernel.org	Broken L
oss-security - Re: CVE request - kernel: xfs: stale data exposure	MLIST	www.openwall.com	Mailing L
git.kernel.org	MISC	git.kernel.org	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Mailing L
SecurityFocus	BUGTRAQ	www.securityfocus.com	Third Pa
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Mailing L
Re: [PATCH] xfsqa: test open_by_handle() on unlinked and freed inode clu	MLIST	oss.sgi.com	Broken L
article.gmane.org 522: Connection timed out	MLIST	article.gmane.org	Broken L
[PATCH] xfsqa: test open_by_handle() on unlinked and freed inode cluster	MLIST	oss.sgi.com	Broken L
oss-security - CVE request - kernel: xfs: stale data exposure	MLIST	www.openwall.com	Mailing L
ASA-2010-291 (RHSA-2010-0723)	CONFIRM	support.avaya.com	Third Pa
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
VMSA-2011-0012.2	CONFIRM	www.vmware.com	Third Pa
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Mailing L
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
Support	REDHAT	www.redhat.com	Broken L
XFS Deleted Inode Local Information Disclosure Vulnerability	BID	www.securityfocus.com	Exploit, T
article.gmane.org 522: Connection timed out	MLIST	article.gmane.org	Broken L
About Secunia Research Flexera	SECUNIA	secunia.com	Broken L
Bug 624923 – CVE-2010-2943 kernel: xfs: validate inode numbers in file handles correctly	CONFIRM	bugzilla.redhat.com	Issue Tra
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Broken L
USN-1057-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Third Pa
Ubuntu update for linux and linux-ec2 - Advisories - Community	SECUNIA	secunia.com	Broken L
USN-1041-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Third Pa
article.gmane.org 522: Connection timed out	MLIST	article.gmane.org	Broken L
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Broken L
Ubuntu update for linux-source-2.6.15 - Secunia.com	SECUNIA	secunia.com	Broken L
article.gmane.org 522: Connection timed out	MLIST	article.gmane.org	Broken L
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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](#).

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