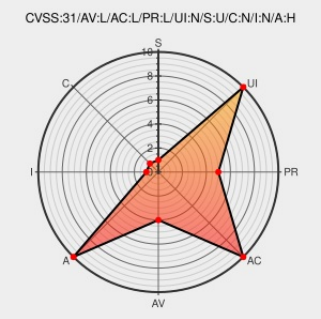
CVE-2012-1090

Published on: 05/17/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:12 AM UTC

CVE-2012-1090

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



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

The cifs_lookup function in fs/cifs/dir.c in the Linux kernel before 3.2.10 allows local users to cause a denial of service (OOPS) via attempted access to a special file, as demonstrated by a FIFO.

CVE-2012-1090 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
798293 – (CVE-2012-1090) CVE-2012-1090 kernel: cifs: dentry refcount leak when opening a FIFO on lookup leads to panic	Issue Tracking, Patch, Third Party Advisory, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=798293

on unmount		
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2012:0531
[security-announce] SUSE-SU-2012:0554-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2012:0554
oss-security - Re: CVE request -- kernel: cifs: dentry refcount leak when opening a FIFO on lookup leads to panic on unmount	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20120228 Re: CVE request -- kernel: cifs: dentry refcount leak when opening a FIFO on lookup leads to panic on unmount
No Description Provided	Third Party Advisory rhn.redhat.com Inactive Link Not Archived	REDHAT RHSA-2012:0481
	Mailing List Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.2.10
About Secunia Research | Flexera	Broken Link secunia.com Depreciated Link text/plain	SECUNIA 48842
cifs: fix dentry refcount leak when opening a FIFO on lookup · torvalds/linux@88d7d4e · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/88d7d4e4a439f32acc56a6d860e415ee71d3df08
About Secunia Research | Flexera	Broken Link secunia.com Depreciated Link text/plain	SECUNIA 48964
[security-announce] SUSE-SU-2012:0616-1: important: Security update for	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SU-2012:0616

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	All	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating System	Redhat	Enterprise Mrg	2.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp2	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All

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

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

cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_high_availability_extension:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_high_availability_extension:11:sp2:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_high_availability_extension:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_high_availability_extension:11:sp2:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:vmware:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:vmware:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:-:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:vmware:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:vmware:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→