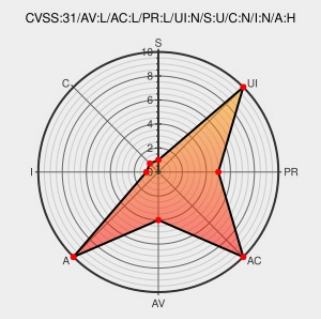
CVE-2012-1146

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

Last Modified on: 02/13/2023 04:33:00 AM UTC

CVE-2012-1146

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

The mem_cgroup_usage_unregister_event function in mm/memcontrol.c in the Linux kernel before 3.2.10 does not properly handle multiple events that are attached to the same eventfd, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by registering memory threshold events.

CVE-2012-1146 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
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=371528caec553785c37f73fa3926ea0de84f986f

	Inactive Link Not Archived	
[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: mm: memcg: unregistring of events attached to the same eventfd can lead to oops	Exploit Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20120307 Re: CVE request -- kernel: mm: memcg: unregistring of events attached to the same eventfd can lead to oops
mm: memcg: Correct unregistring of events attached to the same eventfd · torvalds/linux@371528c · GitHub	Exploit Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/371528caec553785c37f73fa3926ea0de84f986f
Bug 800813 – CVE-2012-1146 kernel: mm: memcg: unregistring of events attached to the same eventfd can lead to oops	Exploit Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=800813
	Mailing List Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.2.10
IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	XF kernel-memcg-dos(73711)
About Secunia Research | Flexera	Broken Link secunia.com Depreciated Link text/plain	SECUNIA 48964
[SECURITY] Fedora 16 Update: kernel-3.2.10-3.fc16	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2012-3712
Security Advisory SA48898 - SUSE update for kernel - Secunia	Broken Link web.archive.org text/html	SECUNIA 48898

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Fedoraproject	Fedora	16	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp2	All	All
Operating System	Suse	Linux Enterprise High Availability Extension	11	sp2	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	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All

cpe:2.3:o:fedoraproject:fedora:16:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:16:*:*:*:*:*:*:*:

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

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

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

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

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

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

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: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→

© CVE.report 2023 |
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 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