



CVE-2009-0745

Published on: 02/27/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:28 PM UTC

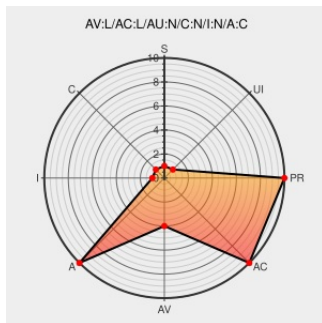
CVE-2009-0745

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

The `ext4_group_add` function in `fs/ext4/resize.c` in the Linux kernel 2.6.27 before 2.6.27.19 and 2.6.28 before 2.6.28.7 does not properly initialize the group descriptor during a resize (aka `resize2fs`) operation, which might allow local users to cause a denial of service (OOPS) by arranging for crafted values to be present in available memory.

CVE-2009-0745 has been assigned by [M](#) cve@mitre.org to track the vulnerability

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
Debian -- Security Information -- DSA-1749-1 linux-2.6	www.debian.org Deprecated Link text/html	DEBIAN DSA-1749
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-0509
Debian update for linux-2.6.24 - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 34981
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20091120 VMSA-2009-0016 VMware vCenter and ESX update release and VMA patch release address multiple security issue in third party components

404: File not found	kernel.org text/plain Inactive Link Not Archived	 CONFIRM kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.27.19
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	 CONFIRM git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=fdff73f094e7220602cc3f8959c7230517976412
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2009-3316
404: File not found	kernel.org text/plain Inactive Link Not Archived	 CONFIRM kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.28.7
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10942
Red Hat update for kernel - Secunia.com	web.archive.org text/html	 SECUNIA 36562
12433 – Oops while resizing an ext4 LVM2 volume	bugzilla.kernel.org text/html	 CONFIRM bugzilla.kernel.org/show_bug.cgi?id=12433
USN-751-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-751-1
Debian -- Security Information -- DSA-1787-1 linux-2.6.24	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1787
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:7765
Debian update for linux-2.6 - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 34394
VMSA-2009-0016.1	www.vmware.com text/html	 CONFIRM www.vmware.com/security/advisories/VMSA-2009-0016.html
rhn.redhat.com Red Hat Support	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2009:1243
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	 SECUNIA 37471
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
Operating System	Linux	Linux Kernel	2.6.27	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.1	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.27.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.28	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.5	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.28.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.27	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.27.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.28	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.1	All	All	All
Operating	Linux	Linux Kernel	2.6.28.2	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.28.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.6	All	All	All
	cpe:2.3:o:linux:linux_kernel:2.6.27:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.1:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.10:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.11:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.12:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.13:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.14:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.15:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.16:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.17:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.18:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.2:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.3:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.4:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.5:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.6:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.7:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.8:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.27.9:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.28:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.28.1:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.28.2:*:*:*:*:*:					
	cpe:2.3:o:linux:linux_kernel:2.6.28.3:*:*:*:*:*:					

cpe:2.3:o:linux:linux_kernel:2.6.28.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.15:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.16:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.17:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.18:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.27.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.28.5:*****:

cpe:2.3:o:linux:linux_kernel:2.6.28.6:*****:*

← 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 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](#)