

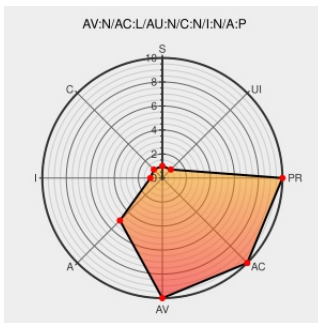


CVE-2005-2099

Published on: 08/22/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2005-2099

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The Linux kernel before 2.6.12.5 does not properly destroy a keyring that is not instantiated properly, which allows local users or remote attackers to cause a denial of service (kernel oops) via a keyring with a payload that is not empty, which causes the creation to fail, leading to a null dereference in the keyring destructor.

CVE-2005-2099 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL oval.org.mitre.oval:def:9079](#)

Linux Kernel Non-Zero Keyring Local Denial of Service Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID 14517](#)

Secunia - Advisories - Linux Kernel Multiple Denial of Service Vulnerabilities

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 16355](#)

Linux Kernel Keyring Destruction Error Lets Local Users Deny Service - SecurityTracker

[securitytracker.com](#)
[text/html](#)

[SECTrack 1014644](#)

SecurityFocus

[www.securityfocus.com](#)

[FEDORA FLSA:157459-3](#)

	text/html	
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:514
Secunia - Advisories - Red Hat update for kernel	Vendor Advisory web.archive.org text/html	 SECUNIA 17073
USN-169-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-169-1
	kernel.org text/plain	 CONFIRM kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.12.5
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRAKE MDKSA-2005:220

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	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All

Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11_rc1_bk6	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	386	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_xeon	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4	All

System							
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4_smp	All	
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc	All	
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc_smp	All	
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All	
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All	
Operating System	Linux	Linux Kernel	2.6.0	All	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test1	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test10	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test11	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test2	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test3	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test4	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test5	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test6	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test7	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test8	All	All	
Operating System	Linux	Linux Kernel	2.6.0	test9	All	All	
Operating System	Linux	Linux Kernel	2.6.1	All	All	All	
Operating System	Linux	Linux Kernel	2.6.1	rc1	All	All	
Operating System	Linux	Linux Kernel	2.6.1	rc2	All	All	
Operating System	Linux	Linux Kernel	2.6.10	All	All	All	
Operating System	Linux	Linux Kernel	2.6.10	rc2	All	All	
Operating System	Linux	Linux Kernel	2.6.11	All	All	All	

System						
Operating System	Linux	Linux Kernel	2.6.11	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.11	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11_rc1_bk6	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.6	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.7	rc1	All	All
Operating	Linux	Linux Kernel	2.6.8	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.8	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.8	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	386	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	686_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_k8_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	amd64_xeon	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	k7_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power3_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	power4_smp	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc	All
Operating System	Linux	Linux Kernel	2.6.8.1.5	All	powerpc_smp	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6_test9_cvs	All	All	All
cpe:2.3::linux:linux_kernel:2.6.0-*****.*						

cpe:2.3:o:linux:linux_kernel:2.6.0:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test1:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test10:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test11:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test2:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test3:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test4:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test5:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test6:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test7:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test8:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.0:test9:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.1:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.10:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc2:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc3:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc4:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.1:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.2:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.3:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.4:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.5:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.6:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.7:~::~:
cpe:2.3:o:linux:linux_kernel:2.6.11.8:~::~:

cpe:2.3:o:linux:linux_kernel:2.6.11_rc1_bk6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.6:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:386:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:686:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:686_smp:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_k8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_k8_smp:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_xeon:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7_smp:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3_smp:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power4:*****:

cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:power4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:power4_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:powerpc:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:powerpc_smp:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test10:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test11:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test5:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test6:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test7:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test8:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.0:test9:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.1:rc1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.1:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc2:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc3:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:rc4:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.11.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11_rc1_bk6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.6:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.7:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:386:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:686:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:686_smp:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:amd64:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5:*:amd64_k8:*****:

cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_k8_smp:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:amd64_xeon:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:k7_smp:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power3_smp:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power4:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:power4_smp:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:powerpc:****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1.5*:powerpc_smp:****:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:****:
cpe:2.3:o:linux:linux_kernel:2.6_test9_cvs:****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)