



CVE-2006-1859

Published on: 05/11/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:59 PM UTC

CVE-2006-1859

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Memory leak in `__setlease` in `fs/locks.c` in Linux kernel before 2.6.16.16 allows attackers to cause a denial of service (memory consumption) via unspecified actions related to an "uninitialised return value," aka "slab leak."

CVE-2006-1859 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Linux Kernel
__SetLease Local
Denial of Service
Vulnerability

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

[BID 18033](#)

Advisories - Mandriva
Linux

[www.mandriva.com](#)
[text/html](#)

[MANDRIVA MDKSA-2006:123](#)

Ubuntu update for
kernel - Advisories -
Secunia

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

[SECUNIA 20716](#)

IBM X-Force
Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF linux-locks-setlease-dos\(26438\)](#)

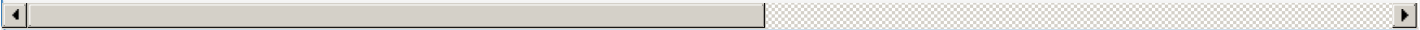
Security
Announcement

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

[SUSE SUSE-SA:2006:042](#)

	Inactive Link Not Archived	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1767
	www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX 2006-0028
Mandriva update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 21045
SUSE update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 21179
usn/usn-302-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	UBUNTU USN-302-1
No Description Provided	www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=commi
Linux Kernel "lease_init()" Denial of Service Vulnerability - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 20083
No Description Provided	www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/git/?p=linux/kernel/git/stable/linux-2.6.16.y.git;a=blobdiff;h=aa7f66091823dde953e15895dc427615701c39c7;hp=e75ac3

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	2.6.16.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.16.15	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.16.15:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.16.15:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [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](#)