



CVE-2011-1767

Published on: 06/13/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:19:00 AM UTC

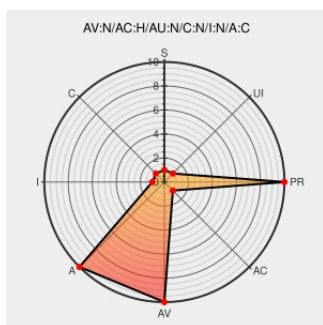
CVE-2011-1767

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

net/ipv4/ip_gre.c in the Linux kernel before 2.6.34, when ip_gre is configured as a module, allows remote attackers to cause a denial of service (OOPS) by sending a packet during module loading.

CVE-2011-1767 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

HIGH

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

gre: fix netns vs proto
registration ordering ·
torvalds/linux@c2892f0 ·
GitHub

[Exploit](#)
[Patch](#)
[github.com](#)
[text/html](#)

CONFIRM
github.com/torvalds/linux/commit/c2892f02712e9516d72841d5c019ed6916329794

Bug 702303 – CVE-2011-
1767 CVE-2011-1768
kernel: netns vs proto
registration ordering

[bugzilla.redhat.com](#)
[text/html](#)

CONFIRM bugzilla.redhat.com/show_bug.cgi?id=702303

No Description Provided

[git.kernel.org](#)
[text/html](#)
Inactive Link **Not Archived**

MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=c2892f02712e9516d72841d5c019ed6916329794

oss-security - Re: CVE
requests - kernel network
vulns

MLIST [oss-security] 20110505 Re: CVE requests - kernel network vulns

404 Not Found

ftp.osuosl.org

text/plain

Inactive Link

Not Archived



CONFIRM <ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.34>

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	2.6.33	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.5	All	All	All

Operating System	Linux	Linux Kernel	2.6.33.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.33	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.16	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.17	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.18	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.33.8	All	All	All

Operating System	Linux	Linux Kernel	2.6.33.9	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.33.*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.1:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.10:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.11:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.12:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.13:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.14:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.15:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.16:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.17:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.18:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.19:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.2:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.3:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.4:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.5:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.6:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.7:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.8:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.9:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.1:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.10:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.11:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.12:*:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:linux:linux_kernel:2.6.33.13:*:~::~~::~~::~~::~~::~~::~~::						

cpe:2.3:o:linux:linux_kernel:2.6.33.14:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.15:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.16:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.17:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.18:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.19:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.33.9:*****:
cpe:2.3:o:linux:linux_kernel:*****:

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 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](#)