

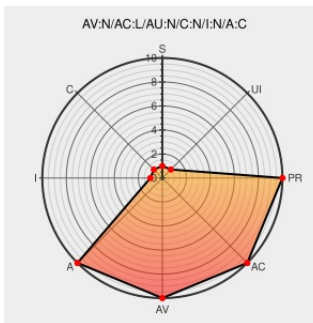


CVE-2005-3848

Published on: 11/26/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-3848

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

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

Memory leak in the icmp_push_reply function in Linux 2.6 before 2.6.12.6 and 2.6.13 allows remote attackers to cause a denial of service (memory consumption) via a large number of crafted packets that cause the ip_append_data function to fail, aka "DST leak in icmp_push_reply."

CVE-2005-3848 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Secunia - Advisories -
Debian update for kernel-
source-2.4.27

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

[X](#) [SECUNIA 19369](#)

Repository / Oval
Repository

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

[OVAL](#) [oval:org.mitre.oval:def:11346](#)

kernel/git/torvalds/linux.git
- Linux kernel source tree

[www.kernel.org](#)
[text/html](#)

[CONFIRM](#) [www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=](#)

Advisories - Mandriva

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

[MANDRIVA MDKSA-2006:072](#)

[PATCH 4/7] [IPV4]: Fix
DST leak in

[marc.info](#)
[text/x-diff](#)

[MLIST](#) [\[linux-kernel\] 20050826 \[PATCH 4/7\] \[IPV4\]: Fix DST leak in icmp_push_re](#)

icmp_push_reply()' - MARC		
Secunia - Advisories - Red Hat update for kernel	web.archive.org text/html	 SECUNIA 18562
Debian update for kernel-source-2.6.8 - Advisories - Secunia	web.archive.org text/html	 SECUNIA 19374
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: kernel various security problems (SUSE-SA:2006:012)	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2006:012
Secunia - Advisories - Ubuntu update for kernel	web.archive.org text/html	 SECUNIA 18203
Secunia - Advisories - Red Hat update for kernel	web.archive.org text/html	 SECUNIA 18510
Debian -- Security Information -- DSA-1018-2 kernel-source-2.4.27	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1018
Secunia - Advisories - SUSE update for kernel	web.archive.org text/html	 SECUNIA 19038
USN-231-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-231-1
'[PATCH] fix dst_entry leak in icmp_push_reply()' - MARC	marc.info text/x-diff	 MLIST [linux-kernel] 20050817 [PATCH] fix dst_entry leak in icmp_push_reply()
No Description Provided	www.kernel.org text/html Inactive Link Not Archived	 CONFIRM www.kernel.org/git/?p=linux/kernel/git/chrisw/stable-queue.git;a=blob;h=1cf41a8a8db3080c9a9243e77c5c447c8e694f87;hb=9c5fcb99af7dst-leak-in-icmp_push_reply.patch
'Re: [PATCH] fix dst_entry leak in icmp_push_reply()' - MARC	marc.info text/html	 MLIST [linux-kernel] 20050818 Re: [PATCH] fix dst_entry leak in icmp_push_reply
Debian -- Security Information -- DSA-1017-1 kernel-source-2.6.8	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1017
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0101
Linux Kernel ICMP_Push_Reply Remote Denial Of Service Vulnerability	cve.report (archive) text/html	 BID 16044
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2006:0140

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	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	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	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating	Linux	Linux Kernel	2.6.12.2	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	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	2.6.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.8.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.9	2.6.20	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating	Linux	Linux Kernel	2.6.11.3	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.10:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*:*:*:*:*:
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:2.6.11.9:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12.1:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12.2:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12.4:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.12.5:*:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.13:*:*:*:*:*:
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:2.6.7:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.8.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*****:
cpe:2.3:o:linux:linux_kernel:2.6.0:*****:
cpe:2.3:o:linux:linux_kernel:2.6.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*****:
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:2.6.11.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13:*****:
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:2.6.7:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.8:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.8.1:*****:*
cpe:2.3:o:linux:linux_kernel:2.6.9:2.6.20:*****:*

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)