

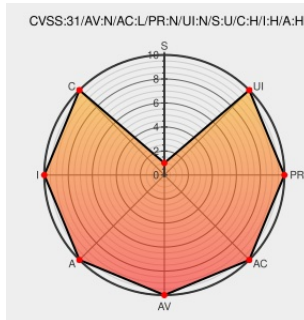


CVE-2015-8787

Published on: 02/07/2016 12:00:00 AM UTC

Last Modified on: 01/19/2023 04:26:00 PM UTC

CVE-2015-8787

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

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

The `nf_nat_redirect_ipv4` function in `net/netfilter/nf_nat_redirect.c` in the Linux kernel before 4.4 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by sending certain IPv4 packets to an incompletely configured interface, a related issue to CVE-2003-1604.

CVE-2015-8787 has been assigned by [@security@debian.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
USN-2890-3: Linux kernel (Raspberry Pi 2) vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-3

USN-2890-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2890-1
netfilter: nf_nat_redirect: add missing NULL pointer check · torvalds/linux@94f9cd8 · GitHub	github.com text/html	 CONFIRM github.com/torvalds/linux/commit/94f9cd81436c85d8c3a318ba92e236ede73752fc
USN-2889-2: Linux kernel (Vivid HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2889-2
Oracle Linux Bulletin - July 2016	web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
oss-security - CVE Request: Linux: NULL pointer dereference netfilter/nf_nat_redirect.c in nf_nat_redirect_ipv4 function	www.openwall.com text/html	 MLIST [oss-security] 20160127 CVE Request: Linux: NULL pointer dereference netfilter/nf_nat_redirect.c in nf_nat_redirect_ipv4 function
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory git.kernel.org text/html	 CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=94f9cd81436c85d8c3a318ba92e236ede73752fc
[SECURITY] Fedora 23 Update: kernel-4.3.4-300.fc23	lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-2f25d12c51
Bug 1300731 – CVE-2015-8787 kernel: Missing NULL pointer check in nf_nat_redirect_ipv4	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1300731
USN-2889-1: Linux kernel vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2889-1
Oracle VM Server for x86 Bulletin - October 2016	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinoct2016-3090547.html
[SECURITY] Fedora 22 Update: kernel-4.3.4-200.fc22	lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-5d43766e33
USN-2890-2: Linux kernel (Wily HWE) vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2890-2
[security-announce] openSUSE-SU-2016:1008-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2016:1008

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	All	All	All	All
Operating System	Linux	Linux Kernel	All	rc8	All	All
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:*:rc8:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		