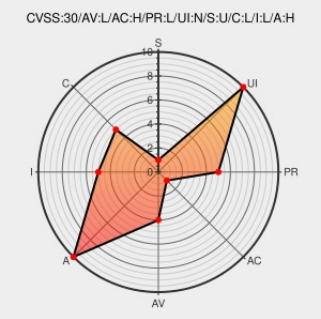
CVE-2015-7990

Published on: 12/28/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

CVE-2015-7990

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

Race condition in the rds_sendmsg function in net/rds/sendmsg.c in the Linux kernel before 4.3.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by using a socket that was not properly bound. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6937.

CVE-2015-7990 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.8 - MEDIUM

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

CVSS2 Score: 5.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2016:0384-1: important:	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0384

Security update for		
[security-announce] SUSE-SU-2015:2350-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2350
USN-2890-3: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-3
	Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.3.3
[security-announce] SUSE-SU-2016:0354-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0354
RDS: fix race condition when sending a message on unbound socket · torvalds/linux@8c7188b · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/8c7188b23474cca017b3ef354c4a58456f68303a
oss-security - Re: CVE-2015-6937 - Linux kernel - NULL pointer dereference in net/rds/connection.c	www.openwall.com text/html	MLIST [oss-security] 20151027 Re: CVE-2015-6937 - Linux kernel - NULL pointer dereference in net/rds/connection.c
USN-2890-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-1
Debian -- Security Information -- DSA-3396-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3396
USN-2886-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2886-1
[security-announce] SUSE-SU-2016:0386-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0386
kernel/git/torvalds/linux.git - Linux kernel source tree	git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8c7188b23474cca017b3ef354c4a58456f68303a
USN-2889-2: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2889-2
Linux Kernel CVE-2015-7990 Incomplete Fix Null Pointer Deference Denial of Service Vulnerability	cve.report (archive) text/html	BID 77340
[security-announce] SUSE-SU-2016:0383-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0383
[security-announce] SUSE-SU-2016:0381-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0381
[security-announce] SUSE-SU-2016:0387-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0387
USN-2887-1: Linux kernel	www.ubuntu.com	UBUNTU USN-2887-1

vulnerabilities | Ubuntu	text/html	
Bug 952384 – VUL-1: CVE-2015-7990: kernel: Incomplete fix for CVE-2015-6937, RDS socket handling	bugzilla.suse.com text/html	CONFIRM bugzilla.suse.com/show_bug.cgi?id=952384
[security-announce] SUSE-SU-2015:2108-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2108
[security-announce] SUSE-SU-2016:0380-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0380
[security-announce] SUSE-SU-2016:2074-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2074
[security-announce] SUSE-SU-2015:2194-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2194
[security-announce] SUSE-SU-2015:2339-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2339
USN-2887-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2887-2
Linux Kernel RDS Null Pointer Dereference Lets Local Users Cause Denial of Service Conditions on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034453
USN-2889-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2889-1
[security-announce] SUSE-SU-2016:0337-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0337
[security-announce] SUSE-SU-2016:0434-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0434
openSUSE-SU-2015:2232-1: moderate: Security update for the Linux Kernel	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2232
[security-announce] SUSE-SU-2016:0335-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0335
CPU Oct 2018	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
USN-2890-2: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-2
USN-2888-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2888-1

LKML: Quentin Casasnovas: [PATCH] RDS: fix race condition when sending a message on unbound socket.	lkml.org text/xml	MLIST [linux-kernel] 20151016 [PATCH] RDS: fix race condition when sending a message on unbound socket.
[security-announce] SUSE-SU-2015:2292-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:2292
Bug 1276437 – CVE-2015-7990 kernel: Race condition when sending message on unbound socket causing NULL pointer dereference	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1276437

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

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→