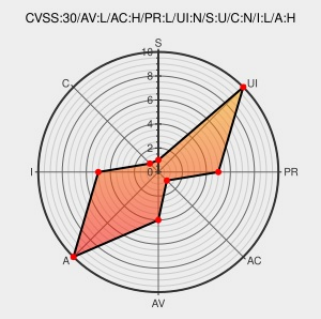
CVE-2013-7446

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

Last Modified on: 11/07/2023 02:18:00 AM UTC

CVE-2013-7446

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



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

Use-after-free vulnerability in net/unix/af_unix.c in the Linux kernel before 4.3.3 allows local users to bypass intended AF_UNIX socket permissions or cause a denial of service (panic) via crafted epoll_ctl calls.

CVE-2013-7446 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5.4 - MEDIUM

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

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2016:2001-1: important: Security update for	lists.opensuse.org, text/html	SUSE SUSE-SU-2016:2001
Linux kernel CVE-2013-7446	cve.report (archive)	BID 77638

Use After Free Denial of Service Vulnerability	text/html	
[security-announce] SUSE-SU-2016:2009-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2009
[PATCH net] af_unix: don't poll dead peers — Linux Network Development	Exploit www.spinics.net text/html	MLIST [netdev] 20150304 [PATCH net] af_unix: don't poll dead peers
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
LKML: Mathias Krause: List corruption on epoll_ctl(EPOLL_CTL_DEL) an AF_UNIX socket	Exploit lkml.org text/xml	MLIST [linux-kernel] 20150913 List corruption on epoll_ctl(EPOLL_CTL_DEL) an AF_UNIX socket
[security-announce] SUSE-SU-2016:1961-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1961
Google Groups	groups.google.com text/html	CONFIRM groups.google.com/forum/#!topic/syzkaller/3twDUI4Cpm8
USN-2890-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-1
oss-security - Re: CVE request - Linux kernel - Unix sockets use after free - peer_wait_queue prematurely freed	www.openwall.com text/html	MLIST [oss-security] 20151118 Re: CVE request - Linux kernel - Unix sockets use after free - peer_wait_queue prematurely freed
Bug 1282688 – CVE-2013-7446 kernel: Unix sockets use after free - peer_wait_queue prematurely freed	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1282688
grsecurity forums • View topic - Consul triggering Kernel crash	forums.grsecurity.net text/html	MISC forums.grsecurity.net/viewtopic.php?f=3&t=4150
[security-announce] SUSE-SU-2016:2010-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2010
[security-announce] SUSE-SU-2016:2005-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2005
[security-announce] SUSE-SU-2016:2002-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2002
[security-announce] openSUSE-SU-2016:1641-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1641
USN-2886-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2886-1

LKML: Linus Torvalds: Re: epoll oops.	Exploit lkml.org text/xml	MLIST [linux-kernel] 20131014 Re: epoll oops.
[security-announce] SUSE-SU-2016:0757-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0757
USN-2889-2: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2889-2
[security-announce] SUSE-SU-2016:0747-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0747
[security-announce] SUSE-SU-2016:2007-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2007
[security-announce] SUSE-SU-2016:0752-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0752
[security-announce] SUSE-SU-2016:0754-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0754
[security-announce] SUSE-SU-2016:0750-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0750
USN-2887-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2887-1
[security-announce] SUSE-SU-2016:1994-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1994
[security-announce] SUSE-SU-2016:1995-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1995
[security-announce] SUSE-SU-2016:2014-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2014
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=7d267278a9ece963d77eefec61630223fce08c6c
[security-announce] SUSE-SU-2016:1102-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:1102
[security-announce] SUSE-SU-2016:0755-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0755
[security-announce] SUSE-SU-2016:0751-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0751
[security-announce] SUSE-SU-2016:0753-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0753
[security-announce] SUSE-	lists.opensuse.org	SUSE SUSE-SU-2016:2074

SU-2016:2074-1: important: Security update for	text/html	
USN-2887-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2887-2
LKML: Peter Zijlstra: eventpoll __list_del_entry corruption (was: perf: use after free in perf_remove_from_context)	Exploit lkml.org text/xml	MLIST [linux-kernel] 20140515 eventpoll __list_del_entry corruption (was: perf: use after free in perf_remove_from_context)
[security-announce] SUSE-SU-2016:2006-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2006
USN-2889-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2889-1
Debian -- Security Information -- DSA-3426-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3426
[security-announce] SUSE-SU-2016:0746-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0746
Linux Kernel Use-After-Free Memory Error in peer_wait_queue() Lets Local Users Cause Denial of Service Conditions on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034557
[security-announce] SUSE-SU-2016:0756-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0756
USN-2890-2: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-2
[security-announce] SUSE-SU-2016:2003-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2003
[security-announce] SUSE-SU-2016:2011-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2011
unix: avoid use-after-free in ep_remove_wait_queue · torvalds/linux@7d26727 · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/7d267278a9ece963d77eefec61630223fce08c6c
USN-2888-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2888-1
[security-announce] SUSE-SU-2016:0745-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0745
[security-announce] SUSE-SU-2016:0911-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0911

[security-announce] SUSE-SU-2016:0749-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0749
[security-announce] SUSE-SU-2016:2000-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2000

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

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 registred 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