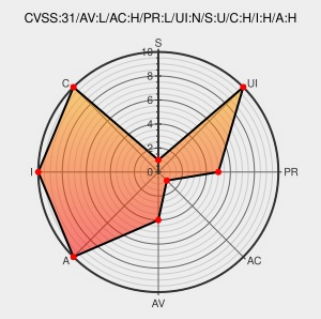
CVE-2015-8543

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

Last Modified on: 06/07/2023 12:47:00 PM UTC

CVE-2015-8543

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



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

The networking implementation in the Linux kernel through 4.3.3, as used in Android and other products, does not validate protocol identifiers for certain protocol families, which allows local users to cause a denial of service (NULL function pointer dereference and system crash) or possibly gain privileges by leveraging CLONE_NEWUSER support to execute a crafted SOCK_RAW application.

CVE-2015-8543 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 6.9 - MEDIUM

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

CVE References

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

vulnerabilities | Ubuntu		
USN-2890-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-1
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0855
USN-2886-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2886-1
Debian -- Security Information -- DSA-3434-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3434
Oracle Linux Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2574
[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-2016:2074-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2074
oss-security - Re: CVE request - Android kernel - IPv6 connect cause a denial of service	www.openwall.com text/html	MLIST [oss-security] 20151209 Re: CVE request - Android kernel - IPv6 connect cause a denial of service
Bug 1290475 – CVE-2015-8543 kernel: IPv6 connect causes DoS via NULL pointer dereference	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1290475
Debian -- Security Information -- DSA-3426-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3426
Google Android Kernel CVE-2015-8543 Null Pointer Deference Local Denial of Service Vulnerability	cve.report (archive) text/html	BID 79698
net: add validation for the socket syscall protocol argument · torvalds/linux@79462ad · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/79462ad02e861803b3840cc782248c7359451cd9
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
Linux Kernel Protocol	www.securitytracker.com	SECTRACK 1034892

Identifier Bug Lets Local Users Cause Denial of Service Conditions on the Target System - SecurityTracker	text/html	
[security-announce] SUSE-SU-2016:0911-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0911
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2584
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=79462ad02e861803b3840cc782248c7359451cd9

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	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→