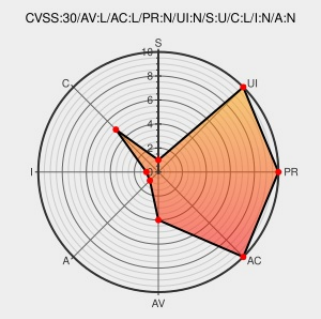
CVE-2015-8575

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

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8575

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



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

The sco_sock_bind function in net/bluetooth/sco.c in the Linux kernel before 4.3.4 does not verify an address length, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism via a crafted application.

CVE-2015-8575 has been assigned by ot security@microfocus.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
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=5233252fce714053f0151680933571a2da9cbfb4
USN-2890-3: Linux kernel (Raspberry Pi 2) vulnerabilities |	www.ubuntu.com text/html	UBUNTU USN-2890-3

Ubuntu		
USN-2890-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-1
USN-2886-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2886-1
	Vendor Advisory www.kernel.org text/x-c	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.3.4
Linux Kernel CVE-2015-8575 Local Information Disclosure Vulnerability	cve.report (archive) text/html	BID 79724
Debian -- Security Information -- DSA-3434-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3434
bluetooth: Validate socket address length in sco_sock_bind(). · torvalds/linux@5233252 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/5233252fce714053f0151680933571a2da9cbfb4
[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
Bug 1292840 – CVE-2015-8575 kernel: information leak in sco_sock_bind()	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1292840
[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
USN-2888-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2888-1
[security-announce] SUSE-SU-2016:0911-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0911
oss-security - Re: CVE Request: Linux Kernel: information leak from getsockname	www.openwall.com text/html	MLIST [oss-security] 20151216 Re: CVE Request: Linux Kernel: information leak from getsockname

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→