

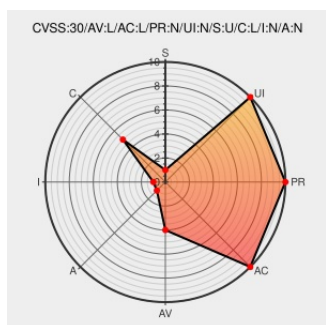


CVE-2015-8575

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/cgi/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 Deprecated 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/5233252f714053f0151680933571a2da9cbfb4
[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

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
<pre>cpe:2.3:o:linux:linux_kernel:*****:::</pre>						
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 registered 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