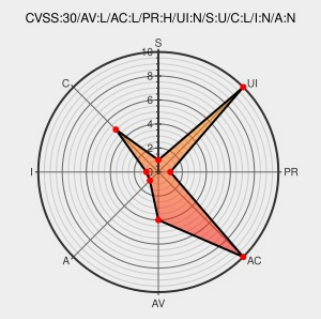
CVE-2015-8569

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

Last Modified on: 11/07/2023 02:28:00 AM UTC

CVE-2015-8569

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



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

The (1) pptp_bind and (2) pptp_connect functions in drivers/net/ppp/pptp.c in the Linux kernel through 4.3.3 do 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-2015-8569 has been assigned by ot security@microfocus.com to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 2.3 - LOW

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

CVSS2 Score: 1.9 - LOW

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

CVE References

Description	Tags	Link
[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-2016:0911-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0911
USN-2890-2: Linux kernel (Wily HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-2
USN-2890-3: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-3
JavaScript is not available.	nitter.domain.glass text/html	MISC twitter.com/grsecurity/statuses/676744240802750464
USN-2886-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2886-1
USN-2890-1: Linux kernel vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2890-1
pptp: verify sockaddr_len in pptp_bind() and pptp_connect() · torvalds/linux@09ccfd2 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/09ccfd238e5a0e670d8178cf50180ea81ae09ae1
Linux Kernel pptp_bind() and pptp_connect() Validation Flaw Lets Local Users View Portions of System Memory on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034549
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=09ccfd238e5a0e670d8178cf50180ea81ae09ae1
Debian -- Security Information -- DSA-3434-1 linux	www.debian.org Depreciated Link text/html	DEBIAN DSA-3434
USN-2888-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2888-1
Bug 1292045 – CVE-2015-8569 kernel: Information leak from getsockname	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1292045
LKML: Dmitry Vyukov: Information leak in pptp_bind	lkml.org text/xml	MLIST [linux-kernel] 20151214 Information leak in pptp_bind
Linux Kernel Multiple Local Information Disclosure Vulnerabilities	cve.report (archive) text/html	BID 79428
oss-security - Re: CVE Request: Linux Kernel: information leak from getsockname	www.openwall.com text/html	MLIST [oss-security] 20151215 Re: CVE Request: Linux Kernel: information leak from getsockname
[security-announce] SUSE-SU-2016:2074-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2074
[SECURITY] Fedora 22 Update: kernel-4.3.4-200.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-5d43766e33

200.fc22

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→