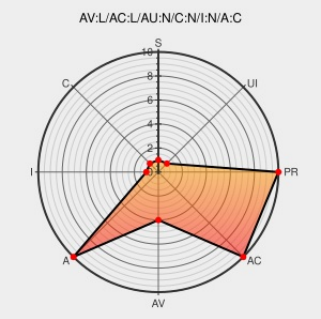
CVE-2012-6657

Published on: 09/28/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:38:00 AM UTC

CVE-2012-6657

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



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

The sock_setsockopt function in net/core/sock.c in the Linux kernel before 3.5.7 does not ensure that a keepalive action is associated with a stream socket, which allows local users to cause a denial of service (system crash) by leveraging the ability to create a raw socket.

CVE-2012-6657 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2015:0812-1: important: Security update for	lists.opensuse.org, text/html	SUSE SUSE-SU-2015:0812
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=3e10986d1d698140747fcfc2761ec9cb64c1d582
oss-security - Re: CVE request Linux kernel: net: guard tcp_set_keepalive against crash	www.openwall.com, text/html	MLIST [oss-security] 20140915 Re: CVE request Linux kernel: net: guard tcp_set_keepalive against crash
'[security bulletin] HPSBGN03285 rev.1 - HP	marc.info, text/html	HP HPSBGN03285

Business Service Manager Virtual Appliance, Multiple Vul' - MARC		
'[security bulletin] HPSBGN03282 rev.1 - HP Business Service Manager Virtual Appliance, Multiple Vuln' - MARC	marc.info text/html	HP HPSBGN03282
net: guard tcp_set_keepalive() to tcp sockets · torvalds/linux@3e10986 · GitHub	Exploit github.com text/html	CONFIRM github.com/torvalds/linux/commit/3e10986d1d698140747fcfc2761ec9cb64c1d582
Bug 1141742 – CVE-2012-6657 Kernel: net: guard tcp_set_keepalive against crash	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1141742
	Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.5.7
[security-announce] SUSE-SU-2015:0652-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2015:0652

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	3.5.1	All	All	All
Operating System	Linux	Linux Kernel	3.5.2	All	All	All
Operating System	Linux	Linux Kernel	3.5.3	All	All	All
Operating System	Linux	Linux Kernel	3.5.4	All	All	All
Operating System	Linux	Linux Kernel	3.5.5	All	All	All
Operating System	Linux	Linux Kernel	3.5.1	All	All	All
Operating System	Linux	Linux Kernel	3.5.2	All	All	All
Operating System	Linux	Linux Kernel	3.5.3	All	All	All

Operating System	Linux	Linux Kernel	3.5.4	All	All	All
Operating System	Linux	Linux Kernel	3.5.5	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Server	10.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	10.0	sp4	All	All
Operating System	Novell	Suse Linux Enterprise Server	11.0	sp1	All	All

cpe:2.3:o:linux:linux_kernel:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.5:*:*:*:*:*:*:*:

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

cpe:2.3:o:novell:suse_linux_enterprise_server:10.0:sp4:*:*:ltss:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:11.0:sp1:*:*:ltss:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:10.0:sp4:*:*:ltss:*:*:*:

cpe:2.3:o:novell:suse_linux_enterprise_server:11.0:sp1:*:*:ltss:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report