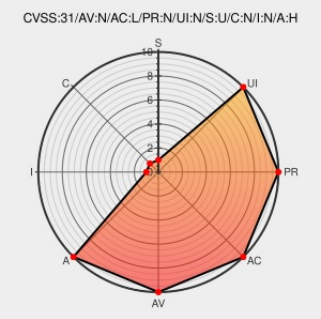
CVE-2016-2070

Published on: 05/02/2016 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:40:00 PM UTC

CVE-2016-2070

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



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

The tcp_cwnd_reduction function in net/ipv4/tcp_input.c in the Linux kernel before 4.3.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via crafted TCP traffic.

CVE-2016-2070 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	Vendor Advisory, git.kernel.org, text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8b8a321ff72c785ed5e8b4cf6eda20b35d427390
tcp: fix zero cwnd in	Patch	CONFIRM

tcp_cwnd_reduction · torvalds/linux@8b8a321 · GitHub	Vendor Advisory github.com text/html	github.com/torvalds/linux/commit/8b8a321ff72c785ed5e8b4cf6eda20b35d427390
1302219 – (CVE-2016-2070) CVE-2016-2070 kernel: potential division by zero in TCP code	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1302219
oss-security - Linux potential division by zero in TCP code	www.openwall.com text/html	MLIST [oss-security] 20160125 Linux potential division by zero in TCP code
	Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.3.5

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→