



CVE-2010-4165

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2010-4165
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-22 13:00:19 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The do_tcp_setsockopt function in net/ipv4/tcp.c in the Linux kernel before 2.6.37-rc2 does not properly restrict TCP_MAXSEG, which allows remote attackers to cause a denial of service (memory consumption) via a crafted packet.

Risk And Classification

Primary CVSS: v2.0 4.9 from nvd@nist.gov

AV:L/AC:L/Au:N/C:N/I:N/A:C

Problem Types: CWE-369 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:L/AC:L/Au:N/C:N/I:N/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Operating System	Linux	Linux Kernel	2.6.37	-	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc1	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References			
Reference	Source		Link
oss-security - Re: CVE request: kernel: possible kernel oops from user MSS	af854a3a-2127-422b-91ae-364da2661108		www
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da2661108		git.ke
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b-91ae-364da2661108		lists.i
SUSE update for kernel - Advisories - Community	af854a3a-2127-422b-91ae-364da2661108		secu
mandriva.com	af854a3a-2127-422b-91ae-364da2661108		www
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108		www
SUSE update for kernel - Advisories - Community	af854a3a-2127-422b-91ae-364da2661108		secu
652508 – (CVE-2010-4165) CVE-2010-4165 kernel: possible kernel oops from user MSS	af854a3a-2127-422b-91ae-364da2661108		bugz
oss-security - CVE request: kernel: possible kernel oops from user MSS	af854a3a-2127-422b-91ae-364da2661108		www
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b-91ae-364da2661108		lists.i
SUSE update for kernel - Advisories - Community	af854a3a-2127-422b-91ae-364da2661108		secu
Malformed Request	af854a3a-2127-422b-91ae-364da2661108		www
Re: possible kernel oops from user MSS — Linux Network Development	af854a3a-2127-422b-91ae-364da2661108		www
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108		www
404: File not found	af854a3a-2127-422b-91ae-364da2661108		www
www.osvdb.org/69241	af854a3a-2127-422b-91ae-364da2661108		www
Linux Kernel <= 2.6.37 Local Kernel Denial of Service - CXSecurity.com	af854a3a-2127-422b-91ae-364da2661108		secu
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	af854a3a-2127-422b-91ae-364da2661108		lists.i
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108		www
[security-announce] SUSE Security Announcement: Realtime Linux Kernel (S	af854a3a-2127-422b-91ae-364da2661108		lists.i
possible kernel oops from user MSS — Linux Network Development	af854a3a-2127-422b-91ae-364da2661108		www
mandriva.com	af854a3a-2127-422b-91ae-364da2661108		www
Linux Kernel <= 2.6.37 rc2 TOP: MAXSEC Kernel Denial DoS - SecurityReason.com	af854a3a-2127-422b-91ae-364da2661108		secu

Linux Kernel < 2.6.37-rc2 TCP_MAXSEG Kernel Panic DOS - SecurityReason.com	af034a3a-2127-422b-91ae-3b40a2b61108	SecurityReason.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)