



CVE-2010-3432

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2010-3432
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-22 13:00:00 UTC
Updated	2023-02-13 04:24:00 UTC
Description	The sctp_packet_config function in net/sctp/output.c in the Linux kernel before 2.6.35.6 performs extraneous initializations c

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All

Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All

References						
Reference			Source		Link	
[security-announce] SUSE Security Announcement: Realtime Linux Kernel (S			SUSE		lists.opensuse.or	
access.redhat.com			REDHAT		www.redhat.com	
Support			REDHAT		www.redhat.com	
Linux Kernel 'sctp_outq_flush()' Denial of Service Vulnerability			BID		www.securityfocu	
kernel/git/torvalds/linux.git - Linux kernel source tree			CONFIRM		git.kernel.org	
Red Hat Customer Portal			MISC		access.redhat.co	
'[PATCH] net: SCTP remote/local Denial of Service vulnerability description and fix' - MARC			MLIST		marc.info	
SecurityFocus			BUGTRAQ		www.securityfocu	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN		www.vupen.com	
Red Hat Customer Portal			MISC		access.redhat.co	
access.redhat.com CVE-2010-3432			MISC		access.redhat.co	
Support			REDHAT		www.redhat.com	
'Re: [oss-security] CVE Request -- Linux/SCTP DoS in sctp_packet_config()' - MARC			MLIST		marc.info	
Red Hat Customer Portal			MISC		access.redhat.co	
404: File not found			CONFIRM		www.kernel.org	
USN-1000-1: Linux kernel vulnerabilities Ubuntu			UBUNTU		www.ubuntu.com	
Support			REDHAT		www.redhat.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN		www.vupen.com	
SUSE update for kernel - Advisories - Community			SECUNIA		secunia.com	
VMSA-2011-0012.2			CONFIRM		www.vmware.cor	
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20			SUSE		lists.opensuse.or	
'[oss-security] CVE Request -- Linux/SCTP DoS in sctp_packet_config()' - MARC			MLIST		marc.info	
About Secunia Research Flexera			SECUNIA		secunia.com	
Debian -- Security Information -- DSA-2126-1 linux-2.6			DEBIAN		www.debian.org	
Red Hat Customer Portal			MISC		access.redhat.co	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN		www.vupen.com	
Red Hat update for kernel - Secunia.com			SECUNIA		secunia.com	
637675 – (CVE-2010-3432) CVE-2010-3432 kernel: sctp: do not reset the packet during sctp_packet_config			CONFIRM		bugzilla.redhat.c	
Red Hat update for kernel - Secunia.com			SECUNIA		secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN		www.vupen.com	

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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