



CVE-2008-3526

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

Summary

CVE	CVE-2008-3526
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-27 20:41:00 UTC
Updated	2023-02-13 02:19:00 UTC
Description	Integer overflow in the sctp_setsockopt_auth_key function in net/sctp/socket.c in the Stream Control Transmission Protocol

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.24	All	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.24.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc4	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc5	All	All	All
Operating System	Linux	Linux Kernel	2.6.25	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.11	All	All	All

Operating System	Linux	Linux Kernel	2.6.25.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.26	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.24	All	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.24	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.24.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.24.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc1	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc4	All	All	All
Operating System	Linux	Linux Kernel	2.6.24_rc5	All	All	All
Operating System	Linux	Linux Kernel	2.6.25	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.13	All	All	All

Operating System	Linux	Linux Kernel	2.6.25.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.25.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.26	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.26.3	All	All	All

References						
Reference			Source		Link	
Linux Kernel 'sctp_setsockopt_auth_key()' Remote Denial of Service Vulnerability			BID		www.securityfocus.co	
git.kernel.org			CONFIRM		git.kernel.org	
Ubuntu update for linux - Secunia.com			SECUNIA		secunia.com	
Support / Security / Advisories // MDVSA-2008:223 Mandriva			MANDRIVA		www.mandriva.com	
CVE-2008-3526 - Red Hat Customer Portal			MISC		access.redhat.com	
460093 – (CVE-2008-3526) CVE-2008-3526 Linux kernel sctp_setsockopt_auth_key() integer overflow			MISC		bugzilla.redhat.com	
Debian update for linux-2.6.24 - Secunia Advisories - Vulnerability Intelligence - Secunia.com			SECUNIA		secunia.com	
Support			REDHAT		www.redhat.com	
USN-659-1: Linux kernel vulnerabilities Ubuntu			UBUNTU		www.ubuntu.com	
IBM X-Force Exchange			XF		exchange.xforce.ibmco	
Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com			SECUNIA		secunia.com	
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20			SUSE		lists.opensuse.org	
git.kernel.org			MISC		git.kernel.org	
Red Hat Customer Portal			MISC		access.redhat.com	
Debian -- Security Information -- DSA-1636-1 linux-2.6.24			DEBIAN		www.debian.org	
oss-security - CVE-2008-3526 Linux kernel sctp_setsockopt_auth_key() integer overflow			MLIST		www.openwall.com	
CVE Program record			CVE.ORG		www.cve.org	
NVD vulnerability detail			NVD		nvd.nist.gov	

Vendor Comments And Credit

Organization	Published	Contributor	Statement
--------------	-----------	-------------	-----------

Red Hat	2009-01-15	Tomas Hoger	This issue did not affect the versions of Linux kernel as shipped with Red Hat Enterprise Linux
---------	------------	-------------	---

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