



# CVE-2008-4445

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

## Summary

|                 |                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2008-4445                                                                                                            |
| State           | PUBLISHED                                                                                                                |
| Assigner        | mitre                                                                                                                    |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                             |
| Published       | 2008-10-06 19:54:36 UTC                                                                                                  |
| Updated         | 2026-04-23 00:35:47 UTC                                                                                                  |
| Description     | The sctp_auth_ep_set_hmacs function in net/sctp/auth.c in the Stream Control Transmission Protocol (sctp) implementation |

## Risk And Classification

Primary CVSS: v2.0 4.7 from nvd@nist.gov

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

Problem Types: CWE-200 | n/a

## CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

None

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product      | Version | Update | Edition | Language |
|------------------|--------|--------------|---------|--------|---------|----------|
| Operating System | Linux  | Linux Kernel | 2.2.27  | All    | All     | All      |

|                  |                       |                              |           |     |     |     |
|------------------|-----------------------|------------------------------|-----------|-----|-----|-----|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.4.36    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.4.36.1  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.4.36.2  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.4.36.3  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.4.36.4  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.4.36.5  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.4.36.6  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6       | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc1 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc2 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc3 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc4 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc5 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc6 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.18    | rc7 | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.19.4  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.19.5  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.19.6  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.19.7  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.20.16 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.20.17 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.20.18 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.20.19 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.20.20 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.20.21 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.21.5  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.21.6  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.21.7  | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22    | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.10 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.11 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.12 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.13 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.14 | All | All | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.15 | All | All | All |

|                  |                       |                              |            |     |        |     |
|------------------|-----------------------|------------------------------|------------|-----|--------|-----|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.17  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.18  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.19  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.2   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.20  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.21  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.22  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.8   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22.9   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22_rc1 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.22_rc7 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23     | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.10  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.11  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.12  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.13  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.15  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.16  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.17  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.8   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23.9   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.23_rc1 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24     | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24.1   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24.2   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24.3   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24.4   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24.5   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24.6   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24.7   | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24_rc1 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24_rc4 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.24_rc5 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25     | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25     | All | x86_64 | All |

|                  |                       |                              |           |     |        |     |
|------------------|-----------------------|------------------------------|-----------|-----|--------|-----|
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.1  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.1  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.10 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.10 | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.11 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.11 | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.12 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.12 | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.13 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.15 | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.2  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.2  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.3  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.3  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.4  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.4  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.5  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.5  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.6  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.6  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.7  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.7  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.8  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.8  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.9  | All | All    | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | 2.6.25.9  | All | x86_64 | All |
| Operating System | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | All       | All | All    | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

References

| Reference                                                     |
|---------------------------------------------------------------|
| Support / Security / Advisories / / MDVSA-2008:223   Mandriva |
| 404: File not found                                           |

| Red Hat update for kernel - Secunia Advisories - Vulnerability Intelligence - Secunia.com                                                                                                                                                                                                                       |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------|-------------------------------------------------------------------------------------------------|-----------|---------|------------|-------------|-------------------------------------------------------------------------------------------------|
| Debian update for linux-2.6 - Secunia.com                                                                                                                                                                                                                                                                       |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| '[PATCH 0/2] sctp: additional overflow fixes' - MARC                                                                                                                                                                                                                                                            |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| '[PATCH 2/2] sctp: fix random memory dereference with SCTP_HMAC_IDENT option.' - MARC                                                                                                                                                                                                                           |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| [security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20                                                                                                                                                                                                                                        |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| oss-security - Re: CVE-2008-4113 update: kernel: sctp: fix random memory dereference with SCTP_HMAC_IDENT option                                                                                                                                                                                                |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| oss-security - Re: CVE-2008-4113 update: kernel: sctp: fix random memory dereference with SCTP_HMAC_IDENT option                                                                                                                                                                                                |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| Linux Kernel 'SCTP' Module Multiple vulnerabilities                                                                                                                                                                                                                                                             |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| SecurityTracker.com Archives - Linux Kernel Validation Flaw in sctp_auth_ep_set_hmacs() Lets Local Users Obtain Potentially Sensitive Infor                                                                                                                                                                     |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| Ubuntu update for linux - Secunia.com                                                                                                                                                                                                                                                                           |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| oss-security - Re: CVE-2008-4113 update: kernel: sctp: fix random memory dereference with SCTP_HMAC_IDENT option                                                                                                                                                                                                |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| Debian -- Security Information -- DSA-1655-1 linux-2.6.24                                                                                                                                                                                                                                                       |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| USN-659-1: Linux kernel vulnerabilities   Ubuntu                                                                                                                                                                                                                                                                |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| git.kernel.org                                                                                                                                                                                                                                                                                                  |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| oss-security - CVE-2008-4113 update: kernel: sctp: fix random memory dereference with SCTP_HMAC_IDENT option                                                                                                                                                                                                    |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| Support                                                                                                                                                                                                                                                                                                         |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| CONFIRM: <a href="http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.26.y.git;a=commit;h=d97240552cd98c4b07322f30f66fd9c3ba4171de">http://git.kernel.org/?p=linux/kernel/git/stable/linux-2.6.26.y.git;a=commit;h=d97240552cd98c4b07322f30f66fd9c3ba4171de</a>                                          |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| CVE Program record                                                                                                                                                                                                                                                                                              |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| NVD vulnerability detail                                                                                                                                                                                                                                                                                        |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| <div><div></div><div></div></div>                                                                                                                                                                                                                                                                               |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| Vendor Comments And Credit                                                                                                                                                                                                                                                                                      |              |             |                                                                                                 |           |         |            |             |                                                                                                 |
| <table><tr><th>Organization</th><th>Published</th><th>Contributor</th><th>Statement</th></tr><tr><td>Red Hat</td><td>2009-01-15</td><td>Tomas Hoger</td><td>This issue did not affect the versions of Linux kernel as shipped with Red Hat Enterprise Linux</td></tr></table> <div><div></div><div></div></div> | 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 |
| 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.                                                                                                                                                                                                                                            |              |             |                                                                                                 |           |         |            |             |                                                                                                 |