# CVE-2014-3673

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-3673 |
| **State** | PUBLISHED |
| **Assigner** | redhat |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2014-11-10 11:55:06 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | The SCTP implementation in the Linux kernel through 3.17.2 allows remote attackers to cause a denial of service (system c |

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**Problem Types:** CWE-20 | n/a

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 2.0 | nvd@nist.gov | Primary | 7.8 | | AV:N/AC:L/Au:N/C:N/I:N/A:C |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/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 |

## Vendor Declared Affected Products

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

## References

| Reference | Source |
|---|---|
| [security-announce] SUSE-SU-2015:0812-1: important: Security update for | af854a3a-2127-422b-91a |
| [security-announce] SUSE-SU-2015:0529-1: important: Security update for | af854a3a-2127-422b-91a |
| linux.oracle.com \| ELSA-2014-3087 | af854a3a-2127-422b-91a |
| USN-2418-1: Linux kernel (OMAP4) vulnerabilities \| Ubuntu | af854a3a-2127-422b-91a |
| net: sctp: fix skb_over_panic when receiving malformed ASCONF chunks · torvalds/linux@9de7922 · GitHub | af854a3a-2127-422b-91a |
| Red Hat Customer Portal | af854a3a-2127-422b-91a |
| linux.oracle.com \| ELSA-2014-3089 | af854a3a-2127-422b-91a |
| Linux Kernel CVE-2014-3673 Denial of Service Vulnerability | af854a3a-2127-422b-91a |
| Debian -- Security Information -- DSA-3060-1 linux | af854a3a-2127-422b-91a |
| [security-announce] SUSE-SU-2015:0652-1: important: Security update for | af854a3a-2127-422b-91a |

| | |
|---|---|
| Red Hat Customer Portal | af854a3a-2127-422b-91a |
| About Secunia Research \| Flexera | af854a3a-2127-422b-91a |
| [security-announce] SUSE-SU-2015:0481-1: important: Security update for | af854a3a-2127-422b-91a |
| linux.oracle.com \| ELSA-2014-3088 | af854a3a-2127-422b-91a |
| '[security bulletin] HPSBGN03282 rev.1 - HP Business Service Manager Virtual Appliance, Multiple Vuln' - MARC | af854a3a-2127-422b-91a |
| [security-announce] openSUSE-SU-2015:0566-1: important: kernel update fo | af854a3a-2127-422b-91a |
| USN-2417-1: Linux kernel vulnerabilities \| Ubuntu | af854a3a-2127-422b-91a |
| Bug 1147850 – CVE-2014-3673 kernel: sctp: skb_over_panic when receiving malformed ASCONF chunks | af854a3a-2127-422b-91a |
| kernel/git/torvalds/linux.git - Linux kernel source tree | af854a3a-2127-422b-91a |
| '[security bulletin] HPSBGN03285 rev.1 - HP Business Service Manager Virtual Appliance, Multiple Vul' - MARC | af854a3a-2127-422b-91a |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MITRE |
| Red Hat Customer Portal | MITRE |
| Red Hat Customer Portal | MITRE |
| Red Hat Customer Portal | MITRE |
| Red Hat Customer Portal | MITRE |
| Red Hat Customer Portal | MITRE |
| access.redhat.com \| CVE-2014-3673 | MITRE |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

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



**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**