CVE-2016-9555

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

Summary

CVE	CVE-2016-9555
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-28 03:59:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the fir

Risk And Classification

Problem Types: CWE-125

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	All	All	All	All

References

Reference
Google Groups
[security-announce] SUSE-SU-2016:3183-1: important: Security update for
Linux Kernel Out-Of-Bounds Read Information Disclosure Vulnerability
[security-announce] SUSE-SU-2016:3169-1: important: Security update for
sctp: validate chunk len before actually using it · torvalds/linux@bf911e9 · GitHub
oss-security - CVE Request: Linux: net/sctp: slab-out-of-bounds in sctp_sf_ootb
[security-announce] SUSE-SU-2016:3206-1: important: Security update for
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.8.8
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Linux Kernel Out-of-Bounds Memory Access Error in SCTP Lets Remote Users Deny Service or Obtain Potentially Sensitive Information - Sec

[security-announce] SUSE-SU-2016:3096-1: important: Security update for
[security-announce] SUSE-SU-2016:3113-1: important: Security update for
Google Groups
Bug 1397930 – CVE-2016-9555 kernel: Slab out-of-bounds access in sctp_sf_ootb()
[security-announce] SUSE-SU-2016:3205-1: important: Security update for
[security-announce] SUSE-SU-2016:3116-1: important: Security update for
kernel/git/torvalds/linux.git - Linux kernel source tree
[security-announce] SUSE-SU-2016:3117-1: important: Security update for
[security-announce] SUSE-SU-2016:3197-1: important: Security update for
Broadcom Support Portal
Red Hat Customer Portal
[security-announce] SUSE-SU-2016:3247-1: important: Security update for
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

378250 Virtuozzo Linux Security Update for kernel-tools-libs (VZLSA-2017:0086)

378258 Virtuozzo Linux Security Update for kernel-headers (VZLSA-2017:0307)