CVE-2017-7558

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

Summary

CVE	CVE-2017-7558
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-26 15:29:00 UTC
Updated	2023-02-12 23:31:00 UTC
Description	A kernel data leak due to an out-of-bound read was found in the Linux kernel in inet_diag_msg_sctp{,l}addr_fill() and sctp_

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	4.7	rc1	All	All
Operating System	Linux	Linux Kernel	4.7	rc2	All	All
Operating System	Linux	Linux Kernel	4.7	rc3	All	All
Operating System	Linux	Linux Kernel	4.7	rc4	All	All
Operating System	Linux	Linux Kernel	4.7	rc5	All	All
Operating System	Linux	Linux Kernel	4.7	rc6	All	All
Operating System	Linux	Linux Kernel	4.7	rc7	All	All
Operating System	Linux	Linux Kernel	4.7	rc1	All	All
Operating System	Linux	Linux Kernel	4.7	rc2	All	All
Operating System	Linux	Linux Kernel	4.7	rc3	All	All
Operating System	Linux	Linux Kernel	4.7	rc4	All	All
Operating System	Linux	Linux Kernel	4.7	rc5	All	All
Operating System	Linux	Linux Kernel	4.7	rc6	All	All

Operating System	Linux	Linux Kernel	4.7	rc7	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
Red Hat Customer Portal
oss-sec: CVE-2017-7558: Linux kernel: sctp: out-of-bounds read in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info()
'[PATCH net] sctp: Avoid out-of-bounds reads from address storage' - MARC
Red Hat Customer Portal
Linux Kernel 'sctp_diag.c' Function Flaws Let Local Users Obtain Potentially Sensitive Information from System Memory - SecurityTracker
Debian -- Security Information -- DSA-3981-1 linux
1480266 – (CVE-2017-7558) CVE-2017-7558 kernel: Out of bounds read in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() in SCT
Linux Kernel CVE-2017-7558 Multiple Local Information Disclosure Vulnerabilities
Red Hat Customer Portal
Bug 1480266 – CVE-2017-7558 kernel: Out of bounds read in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() in SCTP stack
CVE-2017-7558 - Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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