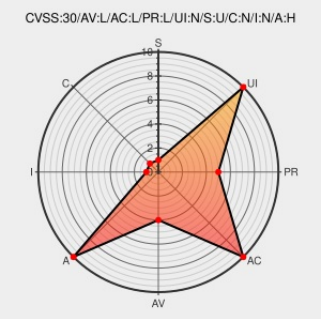
CVE-2018-5803

Published on: 06/12/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:45 PM UTC

CVE-2018-5803

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the "_sctp_make_chunk()" function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can be exploited to cause a kernel crash.

CVE-2018-5803 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Linux Foundation** - **Linux Kernel** version **Before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102.**

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-	Third Party Advisory	DEBIAN DSA-4188

4188-1 linux	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4188
USN-3698-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3698-1
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.15.8
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.1.51
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:1854
USN-3698-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3698-2
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.2.102
Security Advisory SA81331 - Linux Kernel "_sctp_make_chunk()" Denial of Service Vulnerability - Secunia	Third Party Advisory secuniaresearch.flexerasoftware.com text/html	SECUNIA 81331
Computer Security Research - Secunia	Third Party Advisory secuniaresearch.flexerasoftware.com text/html	MISC secuniaresearch.flexerasoftware.com/secunia_research/2018-2/
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.87
[Secunia Research] Linux Kernel Vulnerability - Sending information — Netdev	Mailing List Third Party Advisory www.spinics.net text/html	MLIST [netdev] 20180207 [Secunia Research] Linux Kernel Vulnerability - Sending information
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3083
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2019:0641
Debian -- Security Information -- DSA-4187-1 linux	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4187
[SECURITY] [DLA 1369-1] linux security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180502 [SECURITY] [DLA 1369-1] linux security update
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.25
USN-3654-1: Linux kernel	Third Party Advisory	UBUNTU USN-3654-1

vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	
USN-3654-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3654-2
	Vendor Advisory cdn.kernel.org text/plain	CONFIRM cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.121
USN-3656-1: Linux kernel (Raspberry Pi 2, Snapdragon) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3656-1
USN-3697-2: Linux kernel (OEM) vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3697-2
sctp: skb_over_panic on INIT/INIT_ACK packet sending — Linux SCTP	Mailing List Third Party Advisory www.spinics.net text/html	MLIST [linux-sctp] 20180209 skb_over_panic on INIT/INIT_ACK packet sending
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:2948
USN-3697-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3697-1
kernel/git/stable/linux.git - Linux kernel stable tree	Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=07f2c7ab6f8d0a7e7c5764c4e6cc9c52951b9d9c
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:3096

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	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	Debian	Debian Linux	7.0	All	All	All
Operating	Debian	Debian Linux	8.0	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	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→