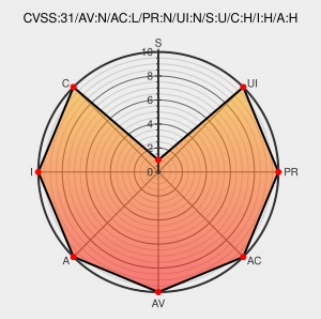
CVE-2019-14897

Published on: 11/29/2019 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:36:00 PM UTC

CVE-2019-14897

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

A stack-based buffer overflow was found in the Linux kernel, version kernel-2.6.32, in Marvell WiFi chip driver. An attacker is able to cause a denial of service (system crash) or, possibly execute arbitrary code, when a STA works in IBSS mode (allows connecting stations together without the use of an AP) and connects to another STA.

CVE-2019-14897 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Red Hat** - **kernel** version **= version kernel-2.6.32**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Kernel Live Patch Security Notice LSN-	packetstormsecurity.com	MISC packetstormsecurity.com/files/156185/Kernel-Live-Patch-Secur

0062-1 ≈ Packet Storm	text/html	1.html
[SECURITY] Fedora 31 Update: kernel-5.3.13-300.fc31 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/MN6MLCN7G7VFTSXSZ
[SECURITY] Fedora 30 Update: kernel-5.3.13-200.fc30 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/D4ISVNIC44SOGXTUBC
USN-4228-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4228-1
USN-4228-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4228-2
USN-4226-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4226-1
[SECURITY] [DLA 2114-1] linux-4.9 security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200302 [SECURITY] [DLA 2114-1] li
USN-4225-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4225-1
Kernel Live Patch Security Notice LSN-0061-1 ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155879/Kernel-Live-Patch-Secur 1.html
USN-4227-2: Linux kernel (Azure) vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4227-2
[security-announce] openSUSE-SU-2020:0336-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0336
USN-4227-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4227-1
USN-4225-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4225-2
[SECURITY] [DLA 2068-1] linux security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200118 [SECURITY] [DLA 2068-1] li
1774879 – (CVE-2019-14897) CVE-2019-14897 kernel: stack-based buffer overflow in add_ie_rates function in drivers/net/wireless/marvell/libertas/cfg.c	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14897

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:linux:linux_kernel:2.6.32:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.32:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→