



CVE-2019-14896

Published on: 11/27/2019 12:00:00 AM UTC

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

CVE-2019-14896

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

A heap-based buffer overflow vulnerability was found in the Linux kernel, version kernel-2.6.32, in Marvell WiFi chip driver. A remote attacker could cause a denial of service (system crash) or, possibly execute arbitrary code, when the lbs_ibss_join_existing function is called after a STA connects to an AP.

CVE-2019-14896 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Red Hat** - kernel 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: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

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	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	Third Party Advisory lists.fedoraproject.org text/html	 MISC lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/D4ISVNIC44SOGXTUBC
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2020:3548
1774875 – (CVE-2019-14896) CVE-2019-14896 kernel: heap-based buffer overflow in lbs_ibss_join_existing function in drivers/net/wireless/marvell/libertas/cfg.c	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1774875
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2019-14896
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] lin
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
December 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20200103-0001/
[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
1774875 – (CVE-2019-14896) CVE-2019-14896 kernel: heap-based buffer overflow in lbs_ibss_join_existing function in drivers/net/wireless/marvell/libertas/cfg.c	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14896
[SECURITY] [DLA 2068-1] linux security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20200118 [SECURITY] [DLA 2068-1] lin

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	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
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	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:*:*:*:its:*:*:*
```

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

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

cpe:2.3:o:fedoraproject:fedora:30:*****:
cpe:2.3:o:fedoraproject:fedora:31:*****:
cpe:2.3:o:fedoraproject:fedora:30:*****:
cpe:2.3:o:fedoraproject:fedora:31:*****:
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:*****:
cpe:2.3:o:redhat:enterprise_linux:6.0:*****:
cpe:2.3:o:redhat:enterprise_linux:6.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)