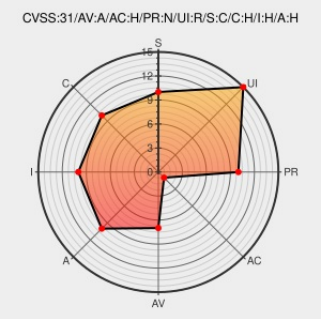
CVE-2019-9503

Published on: 01/16/2020 12:00:00 AM UTC

Last Modified on: 04/18/2022 06:09:00 PM UTC

CVE-2019-9503 - advisory for VU#166939

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



Certain versions of Brcmfmac Driver from Broadcom contain the following vulnerability:

The Broadcom brcmfmac WiFi driver prior to commit a4176ec356c73a46c07c181c6d04039fafa34a9f is vulnerable to a frame validation bypass. If the brcmfmac driver receives a firmware event frame from a remote source, the is_wlc_event_frame function will cause this frame to be discarded and unprocessed. If the driver receives the firmware event frame from the host, the appropriate handler is called. This frame validation can be bypassed if the bus used is USB (for instance by a wifi dongle). This can allow firmware event frames from a remote source to be processed. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.

CVE-2019-9503 has been assigned by cert@cert.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Broadcom** - **brcmfmac WiFi driver** version **commit prior to a4176ec356c73a46c07c181c6d04039fafa34a9f**

CVSS3 Score: 8.3 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.9 - HIGH

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
VU#166939 - Broadcom WiFi chipset drivers contain multiple vulnerabilities	Third Party Advisory US Government Resource kb.cert.org text/html	MISC kb.cert.org/vuls/id/166939/
Bug 1132828 – VUL-1: CVE-2019-9503: kernel-source: brcmfmac frame validation bypass	bugzilla.suse.com text/html	MISC bugzilla.suse.com/show_bug.cgi?id=1132828
1701842 – (CVE-2019-9503) CVE-2019-9503 kernel: brcmfmac frame validation bypass	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1701842
Reverse-engineering Broadcom wireless chipsets	Third Party Advisory blog.quarkslab.com text/html	MISC blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html
CVE-2019-9503	security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2019-9503
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Third Party Advisory git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=a4176ec356c73a46c07c181c6d04039fafa34a9f
CVE-2019-9503 in Ubuntu	people.canonical.com text/html	MISC people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-9503.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Brcmfmac Driver	-	All	All	All
Application	Broadcom	Brcmfmac Driver	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

cpe:2.3:a:broadcom:brcmfmac_driver:-:*:*:*:*:*:*:*:

cpe:2.3:a:broadcom:brcmfmac_driver:-:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@management_sun	IT Risk: SUSE.Linux Kernelに複数の脆弱性 -3/3 CVE-2020-27820 CVE-2019-15126 CVE-2019-9503 CVE-2019-9502 CVE-2019-9501 CVE-2019-9500 CVE-2018-25020	2022-02-11 05:56:24

← Previous ID

Next ID→