



CVE-2019-9500

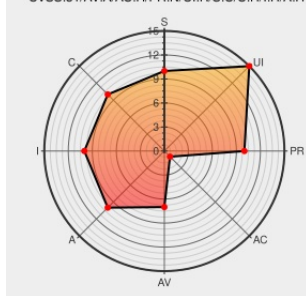
Published on: 01/16/2020 12:00:00 AM UTC

Last Modified on: 01/19/2023 03:53:00 PM UTC

CVE-2019-9500 - advisory for VU#166939

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

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



Certain versions of [Brcmfmac Driver](#) from [Broadcom](#) contain the following vulnerability:

The Broadcom brcmfmac WiFi driver prior to commit 1b5e2423164b3670e8bc9174e4762d297990deff is vulnerable to a heap buffer overflow. If the Wake-up on Wireless LAN functionality is configured, a malicious event frame can be constructed to trigger an heap buffer overflow in the brcmf_wowl_nd_results function. This

vulnerability can be exploited with compromised chipsets to compromise the host, or when used in combination with CVE-2019-9503, can be used remotely. 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-2019-9500 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 1b5e2423164b3670e8bc9174e4762d297990deff**

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 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/
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Third Party Advisory git.kernel.org text/html	 MISC git.kernel.org/linus/1b5e2423164b3670e8bc9174e4762d297990deff
Reverse-engineering Broadcom wireless chipsets	Exploit Third Party Advisory blog.quarkslab.com text/html	 MISC blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html

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
Application	Broadcom	Brcmfmac Driver	-	All	All	All
Application	Broadcom	Brcmfmac Driver	-	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:a:broadcom:brcmfmac_driver:-:*:*:*:*:*:						
cpe:2.3:a:broadcom:brcmfmac_driver:-:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:						

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 →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)