



CVE-2017-6956

Published on: 04/05/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:50 PM UTC

CVE-2017-6956

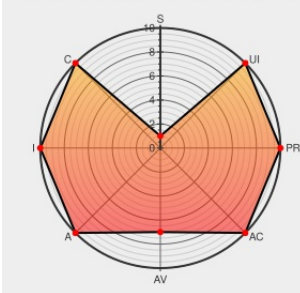
Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)

CVSS:30/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Hardmac Wi-fi Soc](#) from [Broadcom](#) contain the following vulnerability:

On the Broadcom Wi-Fi HardMAC SoC with fbt firmware, a stack buffer overflow occurs when handling an 802.11r (FT) authentication response, leading to remote code execution via a crafted access point that sends a long R0KH-ID field in a Fast BSS Transition Information Element (FT-IE).

CVE-2017-6956 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **8.3 - HIGH**

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

CVE References

Description	Tags	Link
1059 - Broadcom: Stack buffer overflow when handling 802.11r (FT) authentication response - project-zero - Monorail	Third Party Advisory bugs.chromium.org text/html	MISC bugs.chromium.org/p/project-zero/issues/detail?id=1059

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Broadcom	Hardmac Wi-fi Soc	-	All	All	All
Hardware  	Broadcom	Hardmac Wi-fi Soc	-	All	All	All
Operating System	Broadcom	Hardmac Wi-fi Soc Firmware	6.37.34.40	All	All	All
Operating System	Broadcom	Hardmac Wi-fi Soc Firmware	6.37.34.40	All	All	All
cpe:2.3:h:broadcom:hardmac_wi-fi_soc:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:broadcom:hardmac_wi-fi_soc:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:broadcom:hardmac_wi-fi_soc_firmware:6.37.34.40:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:broadcom:hardmac_wi-fi_soc_firmware:6.37.34.40:~::~~::~~::~~::~~::~~::~~:::						