



CVE-2017-6957

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-6957
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-27 14:59:00 UTC
Updated	2017-03-31 11:37:00 UTC
Description	Stack-based buffer overflow in the firmware in Broadcom Wi-Fi HardMAC SoC chips, when the firmware supports CCKM F

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Broadcom	Bcm4339 Soc	-	All	All	All
Hardware	Broadcom	Bcm4339 Soc	-	All	All	All
Operating System	Broadcom	Bcm4339 Soc Firmware	6.37.34.40	All	All	All
Operating System	Broadcom	Bcm4339 Soc Firmware	6.37.34.40	All	All	All

References

Reference	Source	Link
1051 - Broadcom: Stack buffer overflow when parsing CCKM reassociation response - project-zero - Monorail	MISC	bugs.chromium.
Broadcom BCM4339 SoC CVE-2017-6957 Stack-Based Buffer Overflow Vulnerability	BID	www.securityfo
Broadcom Stack Buffer Overflow ≈ Packet Storm	MISC	packetstormsec
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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