



CVE-2017-11120

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

Summary

CVE	CVE-2017-11120
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-28 01:29:00 UTC
Updated	2019-03-13 15:16:00 UTC
Description	On Broadcom BCM4355C0 Wi-Fi chips 9.44.78.27.0.1.56 and other chips, an attacker can craft a malformed RRM neighbor

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Hardware	Broadcom	Bcm4355c0	-	All	All	All
Hardware	Broadcom	Bcm4355c0	-	All	All	All
Operating System	Broadcom	Bcm4355c0 Firmware	9.44.78.27.0.1.56	All	All	All
Operating System	Broadcom	Bcm4355c0 Firmware	9.44.78.27.0.1.56	All	All	All

References

Reference	Source	Link
Malformed Request	BID	v
Android Security Bulletin—September 2017 Android Open Source Project	CONFIRM	s
1289 - Broadcom: OOB write when handling 802.11k Neighbor Report Response - project-zero - Monorail	MISC	t
About the security content of iOS 11 - Apple Support	CONFIRM	s
Broadcom 802.11k Neighbor Report Response Out-Of-Bounds Write ≈ Packet Storm	MISC	f
About the security content of iOS 11 - Apple Support	CONFIRM	s

Apple - Lists.apple.com	APPLE	li
Apple iOS 10.2 - Broadcom Out-of-Bounds Write when Handling 802.11k Neighbor Report Response - iOS remote Exploit	EXPLOIT-DB	v
About the security content of tvOS 11 - Apple Support	CONFIRM	s
About the security content of tvOS 11 - Apple Support	CONFIRM	s
Apple - Lists.apple.com	APPLE	li
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r



No vendor comments have been submitted for this CVE.

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