



CVE-2017-9475

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

Summary

CVE	CVE-2017-9475
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-31 03:29:00 UTC
Updated	2017-08-08 13:57:00 UTC
Description	Comcast XFINITY WiFi Home Hotspot devices allow remote attackers to spoof the identities of Comcast customers via a fo

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Comcast	Xfinity Wifi Hotspot	-	All	All	All
Application	Comcast	Xfinity Wifi Hotspot	-	All	All	All

References

Reference	Source	Link	Tags
CableTap/bastille-17.public-wifi-theft-impersonation.txt at master · BastilleResearch/CableTap · GitHub	MISC	github.com	Third P
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

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