



# CVE-2017-8248

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-8248
<b>State</b>	PUBLIC
<b>Assigner</b>	product-security@qualcomm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-08-16 15:29:00 UTC
<b>Updated</b>	2018-12-07 11:29:00 UTC
<b>Description</b>	A buffer overflow may occur in the processing of a downlink NAS message in Qualcomm Telephony as used in Apple iPhor

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Iphone Os</a>	All	All	All	All

## References

### Reference

- Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, Spoof URLs, Conduct Cross-Site Scripting Attacks, Bypass
- Apple iOS APPLE-SA-2017-07-19-1 Multiple Security Vulnerabilities
- Qualcomm Closed-Source Components Multiple Unspecified Vulnerabilities
- Full Disclosure: APPLE-SA-2017-07-19-1 iOS 10.3.3
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)