



# CVE-2017-16300

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-16300
<b>State</b>	PUBLIC
<b>Assigner</b>	talos-cna@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-11 22:15:00 UTC
<b>Updated</b>	2023-01-23 16:50:00 UTC
<b>Description</b>	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub

## Risk And Classification

**Problem Types:** CWE-121

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Insteon	Insteon Hub	-	All	All	All
Operating System	Insteon	Insteon Hub Firmware	1012	All	All	All

## References

Reference	Source	Link	Tags
TALOS-2017-0483 - Cisco Talos	MISC	<a href="https://talosintelligence.com">talosintelligence.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](#).

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