



CVE-2017-16253

Published on: 03/21/2019 12:00:00 AM UTC

Last Modified on: 12/09/2022 02:33:00 AM UTC

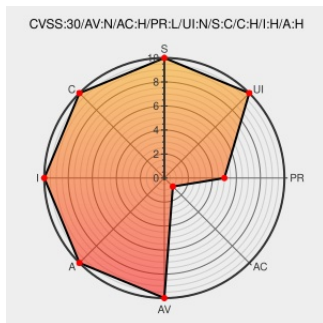
CVE-2017-16253

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Hub](#) from [Insteon](#) contain the following vulnerability:

An exploitable buffer overflow vulnerability exists in the PubNub message handler Insteon Hub 2245-222 - Firmware version 1012 for the cc channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker can send an authenticated HTTP request At 0x9d014dd8 the value for the id key is copied using strcpy to the buffer at \$sp+0x290. This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.

CVE-2017-16253 has been assigned by [Cisco Talos](#) talos-cna@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	HIGH

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
TALOS-2017-0482 - Cisco Talos	CVE	MISC:talosintelligence.com/vulnerability-reports/TALOS-2017-0482

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Insteon	Hub	2245-222	-	All	All
Hardware	Insteon	Hub	2245-222	-	All	All
Operating System	Insteon	Hub Firmware	1012	All	All	All
Operating System	Insteon	Hub Firmware	1012	All	All	All
cpe:2.3:h:insteon:hub:2245-222:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:insteon:hub:2245-222:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:insteon:hub_firmware:1012:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:insteon:hub_firmware:1012:~::~~::~~::~~::~~::~~::~~:::						

Next ID→