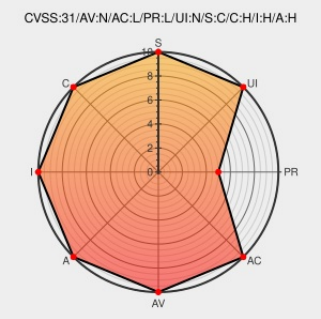
CVE-2017-16293

Published on: Not Yet Published

Last Modified on: 01/23/2023 06:08:00 PM UTC

CVE-2017-16293

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Hub from Insteon contain the following vulnerability:

Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler 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 should send an authenticated HTTP request to trigger this vulnerability. In cmd s_schd, at 0x9d01a010, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.

CVE-2017-16293 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Insteon** - **Hub** version **= Not specified**

CVSS3 Score: 9.9 - CRITICAL

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

CVE References

Description	Tags	Link
TALOS-2017-0483 - Cisco Talos	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2017-0483

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:h:insteon:hub:-:*:*:*:*:*:*:*:

cpe:2.3:o:insteon:hub_firmware:1012:*:*:*:*:*:*:*:

cpe:2.3:h:insteon:insteon_hub:-:*:*:*:*:*:*:*:

cpe:2.3:o:insteon:insteon_hub_firmware:1012:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→