

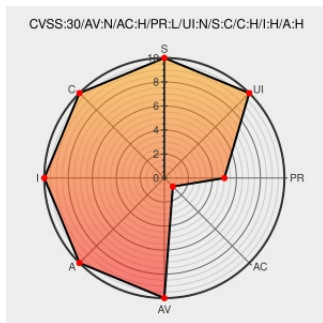


CVE-2017-14446

Published on: 08/02/2018 12:00:00 AM UTC

Last Modified on: 12/14/2022 04:22:00 PM UTC

CVE-2017-14446

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

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

An exploitable stack-based buffer overflow vulnerability exists in Insteon Hub running firmware version 1012. The HTTP server implementation unsafely extracts parameters from the query string, leading to a buffer overflow on the stack. An attacker can send an HTTP GET request to trigger this vulnerability.

CVE-2017-14446 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Cisco](#) **Insteon** - **Insteon** version **Insteon Hub 2245-222** - **Firmware version 1012**

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

CVSS2 Score: **8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
TALOS-2017-0495 - Cisco Talos	Exploit Third Party Advisory www.talosintelligence.com	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2017-0495

comment@cve.report

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
Hardware 	Insteon	Hub	-	All	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:-:*:*:*:*:*:						
cpe:2.3:h:insteon:hub:-:*:*:*:*:*:						
cpe:2.3:o:insteon:hub_firmware:1012:*:*:*:*:*:						
cpe:2.3:o:insteon:hub_firmware:1012:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→