



CVE-2017-6754

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-6754
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-07 06:29:00 UTC
Updated	2019-10-09 23:29:00 UTC
Description	A vulnerability in the web-based management interface of the Cisco Smart Net Total Care (SNTC) Software Collector Appli

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Smart Net Total Care Collector Appliance	3.11	All	All	All
Application	Cisco	Smart Net Total Care Collector Appliance	3.11	All	All	All

References

Reference	Source	Link
Cisco Smart Net Total Care Software Collector Appliance CVE-2017-6754 SQL Injection Vulnerability	BID	www.securi
Cisco Bug: CSCvf07617 - Cisco Smart Net Total Care Portal: SQL Injection Vulnerability in Contracts Details page	CONFIRM	quickview.c
Cisco Smart Net Total Care Contracts Details Page SQL Injection Vulnerability	CONFIRM	tools.cisco.c
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

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

CVE.report and Source URL Uptime Status status.cve.report