



CVE-2017-6656

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

Summary

CVE	CVE-2017-6656
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-13 06:29:00 UTC
Updated	2017-07-08 01:29:00 UTC
Description	A vulnerability in Session Initiation Protocol (SIP) call handling of Cisco IP Phone 8800 Series devices could allow an unaut

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ip Phone 8800 Series	11.0(0.1)	All	All	All
Application	Cisco	Ip Phone 8800 Series	11.0\ (0.1\)	All	All	All
Application	Cisco	Ip Phone 8800 Series	11.0\ (0.1\)	All	All	All

References

Reference	Source
Cisco IP Phone 8800 Series SIP Denial of Service Vulnerability	CC
Cisco IP Phone 8800 Series CVE-2017-6656 Denial of Service Vulnerability	BI
Cisco 8800 Series IP Phones SIP Packet Validation Flaw Lets Remote Users Cause the Target SIP Service to Restart - SecurityTracker	SE
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)