



CVE-2011-0379

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2011-0379
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-25 12:00:00 UTC
Updated	2011-04-09 03:32:00 UTC
Description	Buffer overflow on Cisco Adaptive Security Appliances (ASA) 5500 series devices with software 1.6.x; Cisco TelePresence

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	5500 Series Adaptive Security Appliance	All	All	All	All
Hardware	Cisco	5500 Series Adaptive Security Appliance	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	1.6.0	All	All	All
Application	Cisco	Adaptive Security Appliance Software	1.6.0	All	All	All
Hardware	Cisco	Asa 5500	All	All	All	All
Hardware	Cisco	Asa 5500	All	All	All	All
Application	Cisco	Telepresence Manager	1.2.0.0	All	All	All
Application	Cisco	Telepresence Manager	1.3.2	All	All	All
Application	Cisco	Telepresence Manager	1.4.0	All	All	All
Application	Cisco	Telepresence Manager	1.5.1	All	All	All
Application	Cisco	Telepresence Manager	1.5.2	All	All	All
Application	Cisco	Telepresence Manager	1.6.2	All	All	All
Application	Cisco	Telepresence Manager	1.2.0.0	All	All	All
Application	Cisco	Telepresence Manager	1.3.2	All	All	All
Application	Cisco	Telepresence Manager	1.4.0	All	All	All
Application	Cisco	Telepresence Manager	1.5.1	All	All	All
Application	Cisco	Telepresence Manager	1.5.2	All	All	All

Application	Cisco	Telepresence System Software	1.6.4	All	All	All
Application	Cisco	Telepresence System Software	1.6.5	All	All	All
Application	Cisco	Telepresence System Software	1.6.6	All	All	All
Application	Cisco	Telepresence System Software	1.6.7	All	All	All
Application	Cisco	Telepresence System Software	1.6.8	All	All	All

References

Reference

Cisco TelePresence Endpoint Devices Have Flaws That Let Remote Users Deny Service and Execute Arbitrary Commands and Code - Secur

Cisco Security Advisory: Multiple Vulnerabilities in Cisco TelePresence Recording Server - Cisco Systems

Cisco TelePresence Manager Bugs Let Remote Users Invoke SOAP Methods, Inject Arbitrary Commands, and Execute Arbitrary Code - Secu

Cisco Security Advisory: Multiple Vulnerabilities in Cisco TelePresence Multipoint Switch - Cisco Systems

Cisco TelePresence Recording Server Bugs Let Remote Users Deny Service and Take Full Control of the Target Device - SecurityTracker

Cisco Systems - Redirect to

Cisco TelePresence Multipoint Switch Flaws Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker

Cisco Security Advisory: Multiple Vulnerabilities in Cisco TelePresence Endpoint Devices - Cisco Systems

CVE Program record

NVD vulnerability detail



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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)