



CVE-2006-5233

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

Summary

CVE	CVE-2006-5233
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-11 01:07:00 UTC
Updated	2017-07-20 01:33:00 UTC
Description	Polycom SoundPoint IP 301 VoIP Desktop Phone, firmware version 1.4.1.0040, allows remote attackers to cause a denial of service (CPU usage) by sending a specially crafted SIP INVITE request.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Polycom	Soundpoint Ip 301	1.4.1.0040	All	All	All
Hardware	Polycom	Soundpoint Ip 301	1.4.1.0040	All	All	All

References

Reference	Source	Link
20061004 (0-Day) PolyCom IP-301 VoIP Desktop Phone HTTP server DoS and undocumented TCP port 42	FULLDISC	archives.neohapsis.com
Polycom SoundPoint IP Phones Denial of Service - Advisories - Secunia	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
PolyCom IP-301 VoIP Desktop Phone HTTP Server Denial Of Service Vulnerabilities	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
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.

© [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](#)