



CVE-2007-3321

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

Summary

CVE	CVE-2007-3321
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-06-21 18:30:00 UTC
Updated	2023-11-07 02:00:00 UTC
Description	The Avaya 4602 SW IP Phone (Model 4602D02A) with 2.2.2 and earlier SIP firmware allows remote attackers to cause a d

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Avaya	4602sw Ip Phone	All	All	All	All

References

Reference	Source	Link	Ta
www.sipera.com/index.php		www.sipera.com	
ASA-2007-263 (VIPER-2007-046, VIPER-2007-047, VIPER-2007-048, VIPER-2007-049)	CONFIRM	support.avaya.com	Ve
www.sipera.com/index.php	MISC	www.sipera.com	Ve
Avaya 4602SW SIP Phone Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com	Ve
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
38117	OSVDB	osvdb.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

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](#)