



CVE-2007-5830

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

Summary

CVE	CVE-2007-5830
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-11-05 19:46:00 UTC
Updated	2008-11-15 07:02:00 UTC
Description	Unspecified vulnerability in the administrative interface in Avaya Messaging Storage Server (MSS) 3.1 before SP1, and Me

Risk And Classification

Problem Types: CWE-20 | NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Message Networking	3.1	All	All	All
Application	Avaya	Message Networking	3.1	All	All	All
Application	Avaya	Messaging Storage Server	3.1	All	All	All
Application	Avaya	Messaging Storage Server	3.1	All	All	All

References

Reference	Source	Link	Tag
Avaya Messaging Storage Server and Avaya Message Networking Input Validation Vulnerability	BID	www.securityfocus.com	
Avaya Messaging Products Web Interface Denial of Service - Advisories - Secunia	SECUNIA	secunia.com	Ven
38482	OSVDB	osvdb.org	
ASA-2007-415	CONFIRM	support.avaya.com	Pat
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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](#)