



# CVE-2008-6707

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

## Summary

<b>CVE</b>	CVE-2008-6707
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-04-10 22:00:00 UTC
<b>Updated</b>	2017-08-17 01:29:00 UTC
<b>Description</b>	The Web management interface in Avaya SIP Enablement Services (SES) 3.x and 4.0, as used with Avaya Communicator

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Communication Manager	3.1	All	All	All
Application	Avaya	Communication Manager	3.1.1	All	All	All
Application	Avaya	Communication Manager	3.1.2	All	All	All
Application	Avaya	Communication Manager	3.1.3	All	All	All
Application	Avaya	Communication Manager	3.1.4	All	All	All
Application	Avaya	Communication Manager	3.1.4	sp1	All	All
Application	Avaya	Communication Manager	3.1.4	sp2	All	All
Application	Avaya	Communication Manager	3.1.5	All	All	All
Application	Avaya	Communication Manager	3.1.5	sp0	All	All
Application	Avaya	Communication Manager	3.1	All	All	All
Application	Avaya	Communication Manager	3.1.1	All	All	All
Application	Avaya	Communication Manager	3.1.2	All	All	All
Application	Avaya	Communication Manager	3.1.3	All	All	All
Application	Avaya	Communication Manager	3.1.4	All	All	All
Application	Avaya	Communication Manager	3.1.4	sp1	All	All
Application	Avaya	Communication Manager	3.1.4	sp2	All	All
Application	Avaya	Communication Manager	3.1.5	All	All	All

Application	Avaya	Communication Manager	3.1.5	sp0	All	All
Application	Avaya	Sip Enablement Services	3.0	All	All	All
Application	Avaya	Sip Enablement Services	3.1	All	All	All
Application	Avaya	Sip Enablement Services	3.1.1	All	All	All
Application	Avaya	Sip Enablement Services	4.0	All	All	All
Application	Avaya	Sip Enablement Services	3.0	All	All	All
Application	Avaya	Sip Enablement Services	3.1	All	All	All
Application	Avaya	Sip Enablement Services	3.1.1	All	All	All
Application	Avaya	Sip Enablement Services	4.0	All	All	All

## References

Reference	Source
46599	OSVD
SIP Enablement Service Web Interface Unrestricted Help Access   Research   VoIPshield Systems Inc.	MISC
IBM X-Force Exchange	XF
SIP Enablement Service Web Interface Default Application Execution   Research   VoIPshield Systems Inc.	MISC
SIP Enablement Service Web Interface Objects Folder Script Execution   Research   VoIPshield Systems Inc.	MISC
46600	OSVD
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPE
IBM X-Force Exchange	XF
Avaya SIP Enablement Services Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECU
SIP Enablement Service Web Interface Server Configuration Information Application Execution   Research   VoIPshield Systems Inc.	MISC
Avaya Communication Manager Multiple Security Vulnerabilities	BID
ASA-2008-268	CONF
46598	OSVD
SIP Enablement Service Web Interface States Folder Script Execution   Research   VoIPshield Systems Inc.	MISC
IBM X-Force Exchange	XF
SIP Enablement Service Web Interface Certificate Utility Disclosure   Research   VoIPshield Systems Inc.	MISC
IBM X-Force Exchange	XF
IBM X-Force Exchange	XF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#)