



# CVE-2008-6709

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2008-6709
<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>	Unspecified vulnerability in the Web management interface in Avaya SIP Enablement Services (SES) 3.x and 4.0, as used

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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	<a href="#">Avaya</a>	<a href="#">Communication Manager</a>	3.1.5	sp0	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	3.0	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	3.1	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	3.1.1	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	4.0	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	3.0	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	3.1	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	3.1.1	All	All	All
Application	<a href="#">Avaya</a>	<a href="#">Sip Enablement Services</a>	4.0	All	All	All

## References

Reference	Source	Link
46603	OSVDB	<a href="#">www.o</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.v</a>
Avaya SIP Enablement Services Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">secunia</a>
Avaya Communication Manager Multiple Security Vulnerabilities	BID	<a href="#">www.s</a>
ASA-2008-268	CONFIRM	<a href="#">suppor</a>
IBM X-Force Exchange	XF	<a href="#">exchan</a>
Nothing found for Research Details Php?id=78	MISC	<a href="#">www.v</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

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](#)