



# CVE-2008-2026

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

## Summary

<b>CVE</b>	CVE-2008-2026
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-04-30 14:10:00 UTC
<b>Updated</b>	2018-10-11 20:38:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in WebID/IISWebAgentIF.dll in RSA Authentication Agent 5.3.0.258, and other versi

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rsa	Authentication Agent	All	All	All	All

## References

Reference	Source	Link
SecurityReason - XSS on RSA Authentication Agent login page	SREASON	<a href="#">securityreason.com</a>
RSA Authentication Agent for Web for IIS Cross-Site Scripting - Advisories - Secunia	SECUNIA	<a href="#">secunia.com</a>
RSA Authentication Agent Input Validation Hole in Login Page Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	<a href="#">www.securitytracker.com</a>
SecurityFocus	BUGTRAQ	<a href="#">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**