



# CVE-2008-1204

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

## Summary

<b>CVE</b>	CVE-2008-1204
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-03-08 00:44:00 UTC
<b>Updated</b>	2017-08-08 01:29:00 UTC
<b>Description</b>	Multiple cross-site scripting (XSS) vulnerabilities in the Administration Console in Sun Java System Access Manager 7.1 an

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0	All	linux	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	hp-ux	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	solaris_sparc	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	solaris_x86	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	windows	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.1	All	hp-ux	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.1	All	linux	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.1	All	solaris_sparc	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.1	All	solaris_x86	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.1	All	windows	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0	All	linux	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	hp-ux	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	solaris_sparc	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	solaris_x86	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.0_2005q4	All	windows	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.1	All	hp-ux	All
Application	<a href="#">Sun</a>	<a href="#">Java System Access Manager</a>	7.1	All	linux	All

Application	Sun	<a href="#">Java System Access Manager</a>	7.1	All	solaris_sparc	All
Application	Sun	<a href="#">Java System Access Manager</a>	7.1	All	solaris_x86	All
Application	Sun	<a href="#">Java System Access Manager</a>	7.1	All	windows	All

## References

Reference	Source	Link
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Sun Java System Access Manager Administration Console Multiple Cross-Site Scripting Vulnerabilities	BID	<a href="https://www.securityfocus.com/bid">www.securityfocus.com/bid</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="https://www.vupen.com">www.vupen.com</a>
Sun Java System Access Manager Cross-Site Scripting Vulnerability - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
201251	SUNALERT	<a href="https://sunsolve.sun.com">sunsolve.sun.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</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](https://status.cve.report)