



# CVE-2010-0219

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

## Summary

<b>CVE</b>	CVE-2010-0219
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-10-18 17:00:00 UTC
<b>Updated</b>	2018-10-10 19:51:00 UTC
<b>Description</b>	Apache Axis2, as used in dswsbobje.war in SAP BusinessObjects Enterprise XI 3.2, CA ARCserve D2D r15, and other pro

## Risk And Classification

**Problem Types:** CWE-255

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Axis2	1.3	All	All	All
Application	Apache	Axis2	1.4	All	All	All
Application	Apache	Axis2	1.4.1	All	All	All
Application	Apache	Axis2	1.5	All	All	All
Application	Apache	Axis2	1.5.1	All	All	All
Application	Apache	Axis2	1.5.2	All	All	All
Application	Apache	Axis2	1.6	All	All	All
Application	Apache	Axis2	1.3	All	All	All
Application	Apache	Axis2	1.4	All	All	All
Application	Apache	Axis2	1.4.1	All	All	All
Application	Apache	Axis2	1.5	All	All	All
Application	Apache	Axis2	1.5.1	All	All	All
Application	Apache	Axis2	1.5.2	All	All	All
Application	Apache	Axis2	1.6	All	All	All
Application	Sap	Businessobjects	3.2	All	enterprise_xi	All
Application	Sap	Businessobjects	3.2	All	enterprise_xi	All

## References

Reference	Source	Link
CA ARCServe D2D Axis2 Default Account Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>
CA ARCServe D2D r15 Web Service Servlet Code Execution	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>
SAP BusinessObjects Axis2 Default Admin Password   Rapid7	MISC	<a href="http://www.rapid7.com">www.rapid7.com</a>
Error 404 :(	MISC	<a href="http://retrogod.altervista.it">retrogod.altervista.it</a>
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
CA ARCServe D2D Axis2 Default Account Security Issue - Advisories - Community	SECUNIA	<a href="http://secunia.com">secunia.com</a>
VU#989719 - SAP BusinessObjects Axis2 Default Admin Password	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
70233	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>
<a href="http://spl0it.org/files/talks/source_barcelona10/Hacking%20SAP%20BusinessObject...">spl0it.org/files/talks/source_barcelona10/Hacking%20SAP%20BusinessObject...</a>	MISC	<a href="http://spl0it.org">spl0it.org</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
- Juniper Networks	CONFIRM	<a href="http://kb.juniper.net">kb.juniper.net</a>
<a href="http://service.sap.com/sap/support/notes/1432881">service.sap.com/sap/support/notes/1432881</a>	MISC	<a href="http://service.sap.com">service.sap.com</a>
SAP BusinessObjects Axis2 Default Account Security Issue - Advisories - Community	SECUNIA	<a href="http://secunia.com">secunia.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org/cve). This site includes MITRE data granted under the following [license](http://www.mitre.org/cve).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)