



CVE-2009-0903

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

Summary

CVE	CVE-2009-0903
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-25 01:30:01 UTC
Updated	2026-04-23 00:35:47 UTC
Description	IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.3, and the Feature Pack for Web Services for WAS 6.1 before 6.1.0.15, do not properly validate the SOAPAction header, which allows remote attackers to execute arbitrary code via a crafted SOAP request.

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

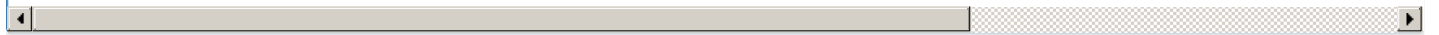
Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	WebSphere Application Server	6.1	All	All	All

Application	IBM	WebSphere Application Server	6.1.0	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.0	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.1	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.10	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.11	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.12	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.13	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.14	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.15	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.16	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.17	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.18	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.19	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.2	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.20	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.21	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.22	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.23	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.24	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.3	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.4	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.5	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.6	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.7	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.8	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.9	All	All	All
Application	IBM	WebSphere Application Server	7.0	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.1	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference				Source		Link
IBM WebSphere Application Server JAX-WS Application Security Bypass Vulnerability				af854a3a-2127-422b-91ae-364da2661108		wv
IBM PK81044: SHIP APAR FIXES FOR LOGW700 FIX PACK 7.0.0.2				af854a3a-2127-422b-91ae-364da2661108		...

IBM PK81944: SHIP APAR FIXES FOR P28W700 FIX PACK 7.0.0.3.	af854a3a-2127-422b-91ae-364da2661108	wv
IBM PK87767: SHIP APAR FIXES FOR JIWO610 COMPID 5655I3550 FIX PACK 6.1.0.25.	af854a3a-2127-422b-91ae-364da2661108	wv
IBM notice: The page you requested cannot be displayed	af854a3a-2127-422b-91ae-364da2661108	wv
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	ex
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv



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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)