CVE-2009-0433

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-0433
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-02-10 22:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Unspecified vulnerability in IBM WebSphere Application Server (WAS) 5.1.x before 5.1.1.19, 6.0.x before 6.0.2.29, and 6.1.

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Application Server	5.1.0	All	All	All

Application	Ibm	Websphere Application Server	5.1.0.2	All	All	All
Application	Ibm	Websphere Application Server	5.1.0.3	All	All	All
Application	Ibm	Websphere Application Server	5.1.0.4	All	All	All
Application	Ibm	Websphere Application Server	5.1.0.5	All	All	All
Application	Ibm	Websphere Application Server	5.1.1	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.1	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.10	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.11	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.12	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.13	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.14	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.15	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.16	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.17	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.18	All	All	All
Application	Ibm	Websphere Application Server	5.1.1.19	All	All	All
Application	Ibm	Websphere Application Server	6.0	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.15	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.5	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.7	All	All	All
Application	Ibm	Websphere Application Server	6.0.1.9	All	All	All
Application	Ibm	Websphere Application Server	6.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.1	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.11	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.13	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.15	All	All	All

Application	Ibm	Websphere Application Server	6.0.2.17	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.19	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.2	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.22	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.23	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.24	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.25	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.27	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.28	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.3	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.4	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.5	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.6	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.7	All	All	All
Application	Ibm	Websphere Application Server	6.0.2.9	All	All	All
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	6.1.0.2	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

Vendor Declared Affected Products

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

References

Reference
IBM notice: The page you requested cannot be displayed
IBM Fix list for IBM WebSphere Application Server V6.1 - United States
IBM X-Force Exchange
IBM Fix list for WebSphere Application Server Version 5.1.1 - United States
IBM Fix list for IBM HTTP Server Version 6.0.2 - United States
IBM WebSphere Application Server Multiple Vulnerabilities
PK67161: ALLOW PK63499 TO BE INSTALLED ON 6.1.0.17 AND PACKAGE 32/64-BIT EXECUTABLES IN THE APPROPRIATE DIRECTO
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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