CVE-2016-5986

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

Summary

CVE	CVE-2016-5986
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-01 01:59:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	IBM WebSphere Application Server (WAS) 7.x before 7.0.0.43, 8.0.x before 8.0.0.13, 8.5.x before 8.5.5.11, 9.0.x before 9.0

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-200 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Application Server	7.0	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.0	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.10	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.11	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.12	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.13	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.14	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.15	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.16	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.17	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.18	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.19	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.2	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.21	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.22	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.23	All	All	All

Application	Ibm	Websphere Application Server	7.0.0.24	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.25	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.27	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.28	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.29	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.31	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.32	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.33	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.34	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.35	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.36	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.37	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.38	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.39	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.4	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.41	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.5	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.6	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.7	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.8	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.9	All	All	All
Application	Ibm	Websphere Application Server	8.0	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.0	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.10	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.11	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.12	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.2	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.4	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.5	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.6	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.7	All	All	All
Application	Ibm	Websphere Application Server	8.0.0.8	All	All	All

Application	Ibm	Websphere Application Server	8.0.0.9	All	All	All
Application	Ibm	Websphere Application Server	8.5.0.0	All	All	All
Application	Ibm	Websphere Application Server	8.5.0.0	-	liberty_profile	All
Application	Ibm	Websphere Application Server	8.5.0.1	-	liberty_profile	All
Application	Ibm	Websphere Application Server	8.5.0.2	-	liberty_profile	All
Application	Ibm	Websphere Application Server	8.5.5.0	-	liberty_profile	All
Application	Ibm	Websphere Application Server	8.5.5.1	-	liberty_profile	All
Application	Ibm	Websphere Application Server	8.5.5.2	-	liberty_profile	All
Application	Ibm	Websphere Application Server	8.5.5.4	All	All	All
Application	Ibm	Websphere Application Server	8.5.5.5	All	All	All
Application	Ibm	Websphere Application Server	8.5.5.6	All	All	All
Application	Ibm	Websphere Application Server	8.5.5.7	All	All	All
Application	Ibm	Websphere Application Server	8.5.5.8	All	All	All
Application	Ibm	Websphere Application Server	8.5.5.9	All	All	All
Application	Ibm	Websphere Application Server	9.0.0.0	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM WebSphere Application Server Response Handing Flaw Lets Remote Users Obtain Potentially Sensitive Information on the Target Syste
IBM WebSphere Application Server CVE-2016-5986 Information Disclosure Vulnerability
IBM Security Bulletin: Potential Information Disclosure vulnerability in WebSphere Application Server (CVE-2016-5986) - United States
IBM notice: The page you requested cannot be displayed
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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