



CVE-2015-0200

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

Summary

CVE	CVE-2015-0200
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-29 15:59:00 UTC
Updated	2019-09-30 16:19:00 UTC
Description	IBM WebSphere Commerce 6.x through 6.0.0.11 and 7.x before 7.0.0.8 IF2 allows local users to obtain sensitive database

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	WebSphere Commerce	6.0.0.0	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.1	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.10	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.11	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.2	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.3	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.4	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.5	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.6	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.7	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.8	All	All	All
Application	ibm	WebSphere Commerce	6.0.0.9	All	All	All
Application	ibm	WebSphere Commerce	7.0	All	All	All
Application	ibm	WebSphere Commerce	7.0.0.1	All	All	All
Application	ibm	WebSphere Commerce	7.0.0.2	All	All	All
Application	ibm	WebSphere Commerce	7.0.0.3	All	All	All
Application	ibm	WebSphere Commerce	7.0.0.4	All	All	All

Application	Ibm	Websphere Commerce	7.0.0.5	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.6	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.7	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.8	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.0	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.1	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.10	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.11	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.2	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.3	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.4	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.5	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.6	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.7	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.8	All	All	All
Application	Ibm	Websphere Commerce	6.0.0.9	All	All	All
Application	Ibm	Websphere Commerce	7.0	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.1	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.2	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.3	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.4	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.5	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.6	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.7	All	All	All
Application	Ibm	Websphere Commerce	7.0.0.8	All	All	All

References
Reference
IBM WebSphere Commerce Database Information Flaw Lets Local Users Obtain Potentially Sensitive Information - SecurityTracker
IBM notice: The page you requested cannot be displayed
IBM Security Bulletin: WebSphere Commerce is affected by an information disclosure vulnerability (CVE-2015-0200) - United States
IBM JR52306: Mandatory cumulative interim fix for WebSphere Commerce Version 7 Feature Pack 7, Fix Pack 8, and Fix Pack 9. - United States
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.

© [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](#)